

Cyclotomic Polynomials

(in the parallel worlds of number theory)

by

Alex Samuel **BAMUNOBA**

Thesis presented in partial fulfilment of the
academic requirements for the degree of
Master of Science
at the University of Stellenbosch



Supervisor : Professor Florian **BREUER**

Department of Mathematical Sciences

University of Stellenbosch

November 21, 2011

Declaration

By submitting this thesis/dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

November 21, 2011

Alex Samuel **BAMUNOBA**

Date

Abstract

It is well known that the ring of integers \mathbf{Z} and the ring of polynomials $A = \mathbf{F}_r[T]$ over a finite field \mathbf{F}_r have many properties in common. It is due to these properties that almost all the famous (multiplicative) number theoretic results over \mathbf{Z} have analogues over A . In this thesis, we are devoted to utilising this analogy together with the theory of Carlitz modules. We do this to survey and compare the analogues of cyclotomic polynomials, the size of their coefficients and cyclotomic extensions over the rational function field $k = \mathbf{F}_r(T)$.

Opsomming

Dit is bekend dat \mathbf{Z} , die ring van heelgetalle en $A = \mathbf{F}_r[T]$, die ring van polinome oor 'n eindige liggaam baie eienskappe in gemeen het. Dit is as gevolg van hierdie eienskappe dat feitlik al die bekende multiplikative resultate wat vir \mathbf{Z} geld, analoë in A het. In hierdie tesis, fokus ons op die gebruik van hierdie analogie saam met die teorie van die Carlitz module. Ons doen dit om 'n oorsig oor die analoë van die siklotomiese polinome, hul koëffisiënte, en siklotomiese uitbreidings oor die rasonele funksie veld $k = \mathbf{F}_r(T)$.

Dedication

This thesis is dedicated to the family of Mr. & Mrs. Nyombi Disan

“If I have been able to see further, it was only because I stood on the shoulders of giants.”

Sir Isaac Newton (1643 – 1727)

Acknowledgements

I would like to express the deepest appreciation to my supervisor, Professor Florian Breuer; for all the support, guidance; providing me with reading material and ideas that gave rise to this thesis. On top of that he's been like a father to me throughout my stay at Stellenbosch.

In addition, I thank Professor Barry Green, the AIMS Director (2010) for his introductory course to algebra delivered at AIMS (2009-10). It has and will always have a lasting effect in my life. I also like to extend my thanks to my lecturers, Doctor Arnold Keet and Professor Stephan Wagner for a series of lectures given in number theory and their friendliness. Thank you for the challenging problems and the *sleepless nights* you gave me. I would also like to thank the AIMS-Stellenbosch scholarship awarding council for having given me this opportunity; it has enabled me to complete my masters degree. I cordially commend this.

While doing my masters, I have appreciated the presence of a number of friends especially my flatmates, John, Juliet, Yusuf and all the AIMS family. I would also like to thank my girl-friend Sharon Raleo, for all the emotional support and encouragement. Lastly, many thanks to my dearest parents, who have given me the freedom to make my own decisions, and occasional phone-calls to check on my well-being while far away from home.

Contents

Declaration	i
Abstract	ii
Opsomming	iii
Dedication	iv
Acknowledgements	v
Introduction	xi
1 Cyclotomic polynomials over \mathbb{Q}	1
1.1 Cyclotomic polynomials	1
1.2 Elementary properties of cyclotomic polynomials	2
1.3 Coefficients of cyclotomic polynomials	4
1.4 Cyclotomic number fields	5
2 Arithmetic of polynomials over \mathbb{F}_r	8
2.1 Polynomials and finite fields	8
2.2 Some properties of A	8
2.3 Euler's and Fermat's little theorems	11
3 Additive polynomials	16

3.1	Basic properties of additive polynomials	16
3.2	Classification of additive polynomials	18
3.3	Properties of the rings $\mathcal{F}[X]$ and $\mathcal{F}\{\tau\}$	19
4	Carlitz module	22
4.1	Valuation theory	22
4.2	The Carlitz exponential	26
4.3	The Carlitz module	30
5	Cyclotomic polynomials over k	36
5.1	Carlitz cyclotomic polynomials	36
5.2	Properties of Carlitz cyclotomic polynomials	38
5.3	Coefficients of Carlitz cyclotomic polynomials	43
5.4	Cyclotomic function fields	51
6	Mahler measure	58
6.1	Elementary properties of Mahler measure	58
6.2	Mahler measure for Carlitz's polynomials	59
6.3	Mahler measure for <i>classical</i> Eisenstein forms	60
7	Conclusion	63
8	Appendix	65
8.1	Algorithms	65
8.2	Eisenstein forms of order one cyclotomic polynomial	67

Bibliography

List of Figures

6.1 Major arc AB of the unit circle shifted to the right by a unit.	61
---	----

List of Tables

5.1	Analogy between the classical and Carlitz cyclotomic polynomials	57
-----	--	----

List of Algorithms

1	Computing $\phi_P(X)$ by a recursion formula	65
2	Computing $\phi_m(X)$ by repeated polynomial division	66
3	Computing $\Phi_m(X)$ by repeated polynomial division	66

Introduction

The ring \mathbf{Z} of integers in \mathbf{Q} and $A := \mathbf{F}_r[T]$, the ring of integers in $k := \mathbf{F}_r(T)$, have many properties in common, for example both are principal ideal domains and, the residue class ring of any non-zero ideal in each is always finite. Both have finite number of units and infinitely many prime elements. In fact, almost all results from multiplicative number theory for \mathbf{Z} have analogues over A . For example, Euler and Fermat's little theorems, Wilson's theorem, the Prime number theorem and Dirichlet's theorem on primes in arithmetic progressions have analogues over the ring A . The analogue to Riemann hypothesis as conjectured by Artin was proved by Hasse in the genus 1 case and by Weil for the general case.

In general, this brief excursion suggests two branches in which number theory is (or can be) studied, these are: elementary number theory and algebraic function field theory (also known as the theory of algebraic curves over finite fields). The former deals with the quotient field \mathbf{Q} of the ring of integers \mathbf{Z} , whereas the latter deals with the quotient field k of the ring of polynomials $\mathbf{F}_r[T]$ over a finite field \mathbf{F}_r . Now, from the arithmetic point of view, k -the field of rational functions in one variable plays a role similar to that of \mathbf{Q} . It is this point of view that we will adopt in the course of this thesis. These approaches of studying number theory are some-times called "*the parallel worlds of number theory*".

This beautiful analogy has been a source of inspiration for new ideas for many years. We undoubtedly continue to anticipate that, a deeper understanding of this analogy could have tremendous consequences in the world of mathematics. In this thesis, we give a concrete background to this analogy, draw the relationships between the two rings \mathbf{Z} , A and show how number theoretic results in the two rings are related. Our treatment of results will be purely arithmetic. All this will be in our effort to give the explicit rational function field analogue to the theory of classical cyclotomic polynomials and cyclotomic extensions.

In order to make the thesis more self-contained, we have devoted chapter 1 to reviewing the classical theory of cyclotomic polynomials and their properties over \mathbf{Q} . We state (without proof) some elementary properties of cyclotomic polynomials over \mathbf{Q} . This is for purposes of introducing the idea of classical cyclotomic polynomials. We also state (without proof)

some known results on coefficients of cyclotomic polynomials, their classification according to order. Towards the end, we give a brief account on the cyclotomic extensions of \mathbf{Q} with emphasis on ramification. This material is intended to equip us with the nature of discussion in chapter 5; that surveys the analogues of these objects over function fields. [18]

In chapter 2, we give a brief but concrete background to the number fields-function fields analogy. In here, we state many properties of the ring A and illustrate how they are analogous to those in \mathbf{Z} . With the help of the chinese remainder theorem, we shall describe the structure of $(A/fA)^*$, the group of units of the quotient ring A/fA , and also state the polynomial versions of some important arithmetic functions. In particular, the Möbius- μ function, the Euler-totient function and their important relationships. As an application of these properties, we state and prove the analogues of Fermat's and Euler's little theorems. We shall also give a brief introduction to the Riemann zeta function for the ring A .

Although there are many similarities between the two fields, we must stress the fact that; there are fundamental differences between these two families (so the analogy is not a perfect one). For example, there exist archimedean absolute values in the number fields case while all those in function fields are non-archimedean [19]. The rings \mathbf{Z} and \mathbf{Q} are essentially unique, as opposed to the polynomial ring A and its field of fractions k , which are respectively isomorphic to many rings and fields. Consequently, the situation of \mathbf{Z} being contained in \mathbf{Q} admits not only one analogue in function fields, but an infinity of them. The additive structures in the two rings are completely different. It is this that motivates us to include chapters on additive polynomials, valuation theory and the Carlitz module. These will help us understand the arithmetic over A better. Therefore, it is salient to keep in mind both aspects: the similarities as well as the fundamental differences between both fields.

In chapter 3, we explore the notion of an additive polynomial over $\mathcal{F}[X]$, but more emphasis will be laid on the polynomial ring $k[X]$ where in this case $k \subseteq \mathcal{F}$. We do this independently in order to develop the theory naturally. We show that, unlike the roots of classical unital polynomial which carry a multiplicative (abelian) group structure, the roots of additive polynomials exhibit an additive (abelian) group structure, more generally an A -module. We explore this structure in detail as it gives an insight on understanding the Carlitz module. We compare and contrast the properties of $\mathcal{F}[X]$ and $\mathcal{F}\{\tau\}$, the twisted polynomial ring.

In chapter 4, we present preliminary material from valuation theory after which we give an analytic approach (but less rigorous) to define the Carlitz exponential $e_C(z)$. This is the function field analogue to the complex exponential $\exp(z)$. We later introduce the theory of the Carlitz module, (in Drinfeld theory, this is a sign normalised rank one Drinfeld module). We mainly follow [10] to describe this module. Algebraically, the Carlitz module is a ring homomorphism $\phi : A \rightarrow \mathbf{C}_\infty\{\tau\}$ that sends each $a \in A$, to $\phi_a \in \mathbf{C}_\infty\{\tau\}$, such that $\phi'_a = a$

and there exists at least one $a \in A$ such that $\phi_a \notin A$. ϕ_a is the a^{th} Carlitz polynomial. This construction is analogous to the classical map $h : \mathbf{Z} \rightarrow \mathbf{C}[X]$ defined by $n \mapsto h_n(X) = X^{|n|}$. We shall give the recursive formula for computing coefficients of ϕ_a .

In chapter 5, we take $m \in A$ and make use of the additive and separability properties of $\phi_m(X)$ to describe the cyclotomic extensions (extensions formed by adjoining roots of $\phi_m(X)$ to k). The roots of these additive polynomials carry a cyclic A -module structure and its generators are the primitive m -torsion points. It is these generators, that we use to construct $\Phi_m(X)$, the m^{th} Carlitz cyclotomic polynomial. $\phi_m(X)$ and $\Phi_m(X)$, are the rational function field analogues to the classical polynomial $h_n(X) = X^{|n|}$ and $\Phi_n(X)$, the n^{th} cyclotomic polynomial. Further still, we explore the elementary properties of $\Phi_m(X)$ over k . We use some of these properties to study coefficients of $\Phi_m(X)$, for example, we show that for any monic irreducible $P \in A$, the prime height of $\Phi_P(X)$ is 1 and its constant term is always P . Using **SAGE**, we explicitly calculate these polynomials to illustrate some of these properties.

Lastly, we calculate the Mahler measure of $\phi_m(X)$ and $\Phi_m(X)$; we also explicitly calculate the Mahler measure of classical Eisenstein-cyclotomic polynomials. We conclude this work with a summary of results obtained, some un-answered problems and our challenges. This thesis is also intended to serve as a basic introduction to the number-function field analogy.

Chapter 1

Cyclotomic polynomials over \mathbf{Q}

Introduction

Let $n \in \mathbf{N}$, the n^{th} unital polynomial $g_n(X) := X^n - 1$ has exactly n distinct zeros called, the n^{th} roots of unity. The set of these n^{th} roots of unity forms a finite multiplicative group which we shall denote by μ_n . In particular, (μ_n, \cdot) is cyclic with its generators as precisely, the primitive n^{th} roots of unity. Therefore, μ_n is an n -torsion group and is explicitly given by,

$$\mu_n = \left\{ \exp\left(\frac{2\pi i}{n}j\right) : j = 0, \dots, n-1 \right\}.$$

We denote the set of all the primitive n^{th} roots of unity by U_n . Adjoining any μ_n -generator ζ_n to \mathbf{Q} , yields a Galois extension $K_n := \mathbf{Q}(\zeta_n)$, called the n^{th} cyclotomic number field. If a is an integer co-prime to n , then there exists an automorphism $\sigma_a \in \text{Gal}(K_n/\mathbf{Q})$ such that $\sigma_a(\zeta_n) = \zeta_n^a \in U_n$, (this a is unique upto modulo n). Moreover, the Galois group of K_n/\mathbf{Q} is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$ and has order $\varphi(n)$, where φ is the Euler-totient function.

1.1 Cyclotomic polynomials

Definition 1.1.1. Let $n \in \mathbf{N}$, the n^{th} cyclotomic polynomial $\Phi_n(X)$ over \mathbf{Q} is the monic polynomial whose roots are precisely all the distinct primitive n^{th} roots of unity. Explicitly,

$$\Phi_n(X) = \prod_{\zeta \in \mu_n: \text{primitive}} (X - \zeta).$$

The n^{th} inverse cyclotomic polynomial $\psi_n(X)$ is one whose roots are the non-primitive n^{th} roots of unity. Since $X^n - 1$ is separable over \mathbf{C} , by definition of $\Phi_n(X)$, its roots are be distinct, and therefore $\Phi_n(X)$ is also separable over \mathbf{C} . We have the following corollary.

Corollary 1.1.2. For all $n \in \mathbf{N}$, we have the identity $\psi_n(X)\Phi_n(X) = X^n - 1$.

In characteristic $p > 0$ fields, we require that $p \nmid n$ for a reason to be given later. However, in \mathbf{Q} (characteristic 0), definition 1.1.1 is just enough. $\Phi_n(X)$ is the minimum polynomial of any primitive n^{th} root and has degree $\varphi(n)$. Here are some of the examples, for small values of n , $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\Phi_{25}(X) = X^{20} + X^{15} + X^{10} + X^5 + 1$, and $\Phi_{32}(X) = X^{16} + 1$. These examples suggest several properties of cyclotomic polynomials over \mathbf{Q} , therefore motivating the following section.

1.2 Elementary properties of cyclotomic polynomials

Here we present properties of $\Phi_n(X)$ over \mathbf{Q} , and highlight differences with \mathbf{F}_p . Recall that, the classical Möbius function is the arithmetic function $\mu : \mathbf{Z} \rightarrow \{0, \pm 1\}$ defined by

$$\mu(n) = \begin{cases} (-1)^s, & \text{if } n \text{ is square free and is product of } s \text{ distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

We have proposition 1.2.1, whose first part is sometimes used as the definition for $\Phi_n(X)$.

Proposition 1.2.1. Let $n \in \mathbf{N}$, then

$$\begin{aligned} X^n - 1 &= \prod_{d|n} \Phi_d(X), \\ \Phi_n(X) &= \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}. \end{aligned}$$

Proposition 1.2.1 enables one to extensively study and prove properties of cyclotomic polynomials over \mathbf{Q} . Also since it relates $g_n(X)$ to its factors $\Phi_d(X)$, where d divides n , we normally use it as a recursive formula for computing $\Phi_n(X)$. Note, although this approach works pretty well for lower values of $n \in \mathbf{N}$, it is still computationally expensive.

Proposition 1.2.2. For each $n \in \mathbf{N}$, $\Phi_n(X) \in \mathbf{Z}[X]$ is monic and irreducible over \mathbf{Q} .

Proof. ([12], Theorem 1, page 195). □

This shows; $\Phi_n(X)$ is the minimum polynomial of any primitive n^{th} root of unity over \mathbf{Q} .

Proposition 1.2.3.

$$\Phi_{np^s}(X) = \begin{cases} \Phi_n(X^{p^s}), & (n, p) \neq 1 \\ \Phi_{np}(X^{p^{s-1}}), & (n, p) = 1. \end{cases}$$

Corollary 1.2.4.

$$\Phi_{np^s}(X) \equiv \begin{cases} \Phi_n(X)^{p^s} & (\text{mod } p), \quad (n, p) \neq 1 \\ \Phi_n(X)^{p^{s-1}(p-1)} & (\text{mod } p), \quad (n, p) = 1. \end{cases}$$

Corollary 1.2.4 is very important in computations involving cyclotomic polynomials over characteristic $p > 0$ fields. Recall, we defined $g_n(X)$ as $g_n(X) = X^n - 1$, so for every $a \in \mathbf{Z}$, $g_{p^s}(a+1) \equiv a^{p^s} \equiv \bar{a} \pmod{p}$ and $\Phi_{p^s}(a+1) \equiv a^{\varphi(p^s)} \equiv 1 \pmod{p}$. In particular, if we set $s = 1$, we obtain $g_p(a+1) = (a+1)^p - 1 \equiv \bar{a} \pmod{p}$ and $\Phi_p(a+1) \equiv a^{p-1} \equiv 1 \pmod{p}$, the Euler and Fermat's little theorems. We will give analogues of this over $k := \mathbf{F}_r(T)$.

If one works in characteristic $p > 0$ field with p dividing n , then by corollary 1.2.4, we observe that $\Phi_n(X)$ is no longer separable. This explains why, when working over finite fields of characteristic $p > 0$, to define $\Phi_n(X)$, we therefore require n and p be co-prime.

Proposition 1.2.5. *If n_0 denotes the largest square-free factor of n , then*

$$\Phi_n(X) = \Phi_{n_0}(X^{\frac{n}{n_0}}).$$

Proposition 1.2.6. *If $n \in \mathbf{N}$ is odd, then $\Phi_{2n}(X) = \Phi_n(-X)$.*

This explains why for odd n , the extensions K_{2n} and K_n are isomorphic i.e. $K_{2n} \cong K_n$.

Proof.

$$\begin{aligned} \Phi_{2n}(X) &= \prod_{d|2n} (X^d - 1)^{\mu(\frac{2n}{d})} = \prod_{d|n} (X^d - 1)^{\mu(\frac{2n}{d})} \prod_{d|n} (X^{2d} - 1)^{\mu(\frac{2n}{2d})} = \prod_{d|n} \left(\frac{X^{2d}-1}{X^d-1} \right)^{\mu(\frac{n}{d})} \\ &= \prod_{d|n} (X^d + 1)^{\mu(\frac{n}{d})} = \prod_{d|n} \left(-((-X)^d - 1) \right)^{\mu(\frac{n}{d})} = (-1)^{\sum_{d|n} \mu(\frac{n}{d})} \Phi_n(-X) = \Phi_n(-X). \end{aligned}$$

□

Proposition 1.2.7 (Reciprocity). *For all $n > 1$, $X^{\varphi(n)}\Phi_n(X^{-1}) = \Phi_n(X)$.*

As a result, for $n > 1$, $\Phi_n(X)$ is palindromic i.e. if $\Phi_n(X) = \sum_{s=0}^{\varphi(n)} a_n(s)X^s$, then

$$\sum_{s=0}^{\varphi(n)} a_n(s)X^{\varphi(n)-s} = X^{\varphi(n)}\Phi_n(X^{-1}) = \Phi_n(X) = \sum_{s=0}^{\varphi(n)} a_n(\varphi(n)-s)X^{\varphi(n)-s}.$$

So if $V_n = \{a_n(s) : 0 \leq s \leq \varphi(n)\}$, then $V_n = \{a_n(n-s) : 0 \leq s \leq \varphi(n)\} = V_n^1$, the set of the coefficients written from the highest degree monomial to the lowest. Therefore, to know $\Phi_n(X)$ explicitly, it suffices to know the $a_n(s)$ for $s = 0, 1, \dots, \frac{\varphi(n)}{2}$.

1.3 Coefficients of cyclotomic polynomials

Looking at the first few examples of cyclotomic polynomials, one can be led to conjecture that the coefficients of cyclotomic polynomials belong to $\{-1, 0, 1\}$. However, this is false, for example, -2 is one of the coefficients of $\Phi_{105}(X)$. In fact, in 1987, Suzuki [21] proved that,

Theorem 1.3.1. *Every integer is a coefficient in some cyclotomic polynomial.*

Let $n \in \mathbf{N}$, the **order** of $\Phi_n(X)$ is the number of distinct odd prime factors of n . For lower orders, cyclotomic polynomials have been given special names, for example; $\Phi_n(X)$ is called **prime** if its order is 1, **binary** if its order is 2, **ternary** if its order is 3, **quaternary** if its order is 4 and **quintic** for order 5. Trivially, we shall classify $\Phi_1(X)$ and $\Phi_{2^s}(X)$ to have order zero.

The **height** of $\Phi_n(X)$ (denoted by $\mathcal{H}(\Phi_n(X))$ or $\mathcal{H}(n)$), is the maximum in absolute value (usual absolute value in \mathbf{R}) of all its coefficients. We denote by V_n , the list of its coefficients. $\Phi_n(X)$ is said to be **flat** if its height is 1, for example $\Phi_1(X)$, $\Phi_4(X)$, $\Phi_{43}(X)$, $\Phi_{104}(X)$. Actually, for $1 \leq n < 105$, $\Phi_n(X)$ is flat, however this does not mean there are no flat cyclotomic polynomials for $n \geq 105$. In fact, it is easy to show that for all primes p , $\Phi_p(X)$ is flat. It is also important to note that, this is not the only class of flat cyclotomic polynomials, there exist other infinite families of flat as well as non-flat cyclotomic polynomials as seen later.

In order to determine $\mathcal{H}(n)$, propositions 1.2.5 and 1.2.6 show that it is enough to consider odd square free composite values of n . If we consider t to be the order $\Phi_n(X)$, then for large values of t , the function $\mathcal{H}(n)$ behaves erratically. So instead of analytically studying $\mathcal{H}(n)$, mathematicians have devoted to suggesting bounds in which the height would lie. For example, P. Erdos showed that $\mathcal{H}(n)$ is not bounded above by any polynomial in n .

Theorem 1.3.2. *For any constant $c > 0$, there exists n such that $\mathcal{H}(n) > n^c$.*

We shall see an analogous statement to be true in the rational function field case. It would also be fruitful to study the arithmetic means of the heights. Since averages tend to smooth out fluctuations, it is reasonable to expect that the mean values $\bar{\mathcal{H}}(n)$ (the average of the heights of the first n cyclotomic polynomials) might behave more regularly than $\mathcal{H}(n)$.

Several papers have studied the values n for which the height $\mathcal{H}(n)$ is large, for-example, Bateman proved an upper bound $\mathcal{H}(n) \leq n^{2^{t-1}}$. Later on he, Pomerance and Vaughan improved the bound to $\mathcal{H}(n) \leq n^{\frac{2^t-1}{t}-1}$ [5]. There is vast literature on coefficients of cyclotomic polynomials, however, for this thesis we shall only concentrate on $\Phi_n(X)$ such that $\mathcal{H}(n)$ is small and try to find if there are analogues over the rational function fields.

In 1883, Migotti made an astounding observation when he showed that, all coefficients of

binary cyclotomic polynomials belonged to $\{0, \pm 1\}$. Lam and Leung [14], showed that for distinct primes p, q , the non-zero coefficients of $\Phi_{pq}(X)$ alternate between -1 and $+1$.

Theorem 1.3.3. *All order zero, one and two cyclotomic polynomials are flat.*

Proof. $\mathcal{H}(2) = \mathcal{H}(1) = 1$. We have $\Phi_p(X) = \frac{X^p-1}{X-1} = 1 + X + \dots + X^{p-1}$, so $\mathcal{H}(p) = 1$. By proposition 1.2.5 and proposition 1.2.6, $\mathcal{H}(2^s p^t) = \mathcal{H}(2p) = \mathcal{H}(p) = 1$. By proposition 1.2.5 and Lam-Leung theorem [14], we have $\mathcal{H}(p^s q^t) = \mathcal{H}(pq) = 1$ and the proof is complete. \square

Bachman [2] gave the first infinite family of flat cyclotomic polynomials of order three. In 2007, Kaplan [13] expanded this family, when he introduced the notion of periodicity. With this, he showed that if $p < q < r$ are primes such that $r \equiv \pm 1 \pmod{pq}$, then $\mathcal{H}(pqr) = 1$.

Theorem 1.3.4 (Periodicity). *Let $2 < p_1 < p_2 < \dots < p_r$ be odd primes, $n = p_1 p_2 \dots p_r$. Let s, t be primes satisfying $n < s < t$ and $s \equiv \pm t \pmod{n}$, then $\mathcal{H}(ns) = \mathcal{H}(nt)$.*

Remark 1.3.5. *It is important to note that the classification according to this periodicity fact is far from complete. For example, there exist flat cyclotomic polynomials of order 3 that are not of this form, a case in point are the polynomials $\Phi_{3 \cdot 7 \cdot 19}(X)$ and $\Phi_{3 \cdot 7 \cdot 23}(X)$ are flat but not of the above form.*

Theorem 1.3.4 suggests that for such primes, increase in order fixes the height. For more about the coefficients and some recent conjectures concerning classification of $\Phi_n(X)$, see [6] and [13]. Lastly, if n_0 denotes the largest odd square free factor of n , then $\mathcal{H}(n) = \mathcal{H}(n_0)$.

1.4 Cyclotomic number fields

In this section, we recall several features from the theory of cyclotomic number fields. This is for purposes of laying a concrete basis for exploring other similarities between k and \mathbf{Q} , the subject of chapter 5. Of course these similarities are centred in the finite (algebraic) extensions of each field. Although we shall restrict ourselves to cyclotomic number fields in this section; the theory is still true for any finite, separable field extensions.

The n^{th} -cyclotomic number field K_n is the extension field formed by adjoining a primitive n^{th} root of unity $\zeta_n \in \mathbf{C}$ to \mathbf{Q} . This was first studied by Gauss in connection with his investigations into constructibility of regular polygons. We have already seen that, K_n is Galois, since it is the splitting field (and therefore normal) for the separable polynomial $g_n(X) = X^n - 1$.

Proposition 1.4.1. *K_n is an abelian extension of \mathbf{Q} of degree $\varphi(n)$.*

Sketch proof. Since the elements of $\text{Gal}(K_n/\mathbf{Q})$ permute the generators ζ_n of K_n , we get a group homomorphism $\rho : \text{Gal}(K_n/\mathbf{Q}) \rightarrow \mathcal{S}_{\varphi(n)}$. If for each $a \in (\mathbf{Z}/n\mathbf{Z})^*$, we define the corresponding Galois element σ_a as $\sigma_a(\zeta_n) = \zeta_n^a$, we see that $\rho : \text{Gal}(K_n/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$.

Irreducibility of $\Phi_n(X)$ over \mathbf{Q} implies that, all the generators of μ_n are \mathbf{Q} -conjugate and therefore ρ , is indeed an epimorphism. The fact that both groups are finite, establishes the isomorphism between $\text{Gal}(K_n/\mathbf{Q})$ and $(\mathbf{Z}/n\mathbf{Z})^*$. Since $(\mathbf{Z}/n\mathbf{Z})^*$ is an abelian group, so is $\text{Gal}(K_n/\mathbf{Q})$. Therefore, K_n is an abelian \mathbf{Q} -extension of degree $\varphi(n)$. \square

There are two important consequences of the action of $\text{Gal}(K_n/\mathbf{Q})$ on U_n . Firstly, σ_{-1} acts as the complex conjugation map on K_n , i.e. $\sigma_{-1}(\zeta_n) = \zeta_n^{-1} = \zeta_n^*$, the complex conjugate. Secondly, if $p \nmid m$, then σ_p is the Artin automorphism for the prime ideal $p\mathbf{Z} \subset \mathbf{Z}$. Using this, we can calculate how ideals in \mathbf{Z} factor in K_n . To understand what is going on, we need to understand the ring of integers \mathcal{O}_n in K_n (recall; \mathcal{O}_n and \mathbf{Z} are both Dedekind domains). Let $p \in \mathbf{Z}$ be a prime, then $p\mathbf{Z}$ is a prime ideal in \mathbf{Z} , and $p\mathcal{O}_n$ is an ideal of \mathcal{O}_n . We can write $p\mathcal{O}_n$ uniquely as a product of powers of prime ideals in \mathcal{O}_n . Let

$$p\mathcal{O}_n = \wp_1^{e_1} \cdots \wp_g^{e_g}, \quad (1.1)$$

be the prime decomposition of $p\mathcal{O}_n$ into distinct prime ideals of \mathcal{O}_n . In fact, for each i , we have $\wp_i \cap \mathbf{Z} = p\mathbf{Z}$, in which case we say that, the prime \wp_i lies above $p\mathbf{Z}$ (or $\wp_i \mid p\mathbf{Z}$) with ramification index $e(\wp_i/p\mathbf{Z}) := e_i$. Since $\wp_i \supseteq p\mathbf{Z}$, the quotient $\mathcal{K}_i := \mathcal{O}_n/\wp_i$ is a finite field extension of the finite field $\mathcal{K} := \mathbf{Z}/p\mathbf{Z}$ for each i . The former is called the residue field of \wp_i with extension degree $f(\wp_i/p\mathbf{Z}) := f_i$ also called the residue (inertia) degree of p in \mathcal{K}_i . It is a standard result for any number field of degree n that,

$$\sum_{i=1}^g e_i f_i = n. \quad (1.2)$$

We say that, K_n/\mathbf{Q} is ramified at $p\mathbf{Z}$ if $e_i > 1$ for some i . If in addition to $e_i > 1$, the e_i 's are co-prime to p for all i , then K_n/\mathbf{Q} is said to be tamely ramified, otherwise K_n is wildly ramified. If there is a unique prime ideal \wp in \mathcal{O}_n lying above $p\mathbf{Z}$ with $f = 1$, i.e. to say $e = \varphi(n)$, then we say that K_n/\mathbf{Q} is totally ramified at $p\mathbf{Z}$ and we have $p\mathcal{O}_n = \wp^{\varphi(n)}$.

We say K_n/\mathbf{Q} is unramified at $p\mathbf{Z}$ if $e_i = 1$ for all i . In particular, if $e_i = f_i = 1$ for all i , then $p\mathbf{Z}$ is said to split completely in K_n/\mathbf{Q} . We say $p\mathbf{Z}$ is inert in K_n if and only if $e = g = 1$ and $f = \varphi(n)$. Much as we have used K_n instead of an arbitrary field in the above discussion; for any Galois extension (K_n in particular), we have $e_i = e$ and $f_i = f$ for all i . Thus, equation 1.2 becomes $efg = \varphi(n)$ and most of the relations above simplify.

In general cyclotomic theory, if $n = p^e$, then K_{p^e} is un-ramified at all primes different from p . To deduce this, we first prove the following **CLAIM**: K_{p^e} is totally ramified at p and the prime ideal in \mathcal{O}_{p^e} lying above $p\mathbf{Z}$ is $\langle \zeta - 1 \rangle$, where ζ is a root to $\Phi_{p^e}(X)$. In this case, if $a \in \mathbf{Z}$ is co-prime to p , then we can always find $b \in \mathbf{Z}$ such that $ab \equiv 1 \pmod{p^e}$. It is clear that $\frac{\zeta^a - 1}{\zeta - 1} \in \mathcal{O}_{p^e}$, we therefore have, $\frac{\zeta - 1}{\zeta^a - 1} = \frac{\zeta^{ab} - 1}{\zeta^a - 1} \in \mathcal{O}_{p^e}$. This implies, $\frac{\zeta^a - 1}{\zeta - 1}$ is a unit in \mathcal{O}_{p^e} . Since

the irreducible polynomial for ζ over \mathbf{Q} is $\Phi_{p^e}(X)$, we have $\widehat{\Phi_{p^e}}(X) := \Phi_{p^e}(X+1)$, as the irreducible polynomial of $\zeta - 1$ (Eisenstein for the prime p , see Appendix 8.1). Its other roots are $\{\zeta^a - 1 : 1 \leq a < p^e, \text{ where } (a, p) = 1\}$. Since $\widehat{\Phi_{p^e}}(0) = \Phi_{p^e}(1) = p$, we have,

$$p = \prod_{a=1, (a,p)=1}^{p^e} (\zeta^a - 1) = \prod_{a=1, (a,p)=1}^{p^e} (\zeta - 1) \frac{(\zeta^a - 1)}{(\zeta - 1)} = (\zeta - 1)^{\phi(p^e)} * \text{unit}.$$

On passing to ideals, we get $p\mathcal{O}_{p^e} = \langle \zeta - 1 \rangle^{\phi(p^e)}$. Since $[K_{p^e} : \mathbf{Q}] = \phi(p^e)$, this can only happen if $\langle \zeta - 1 \rangle \subset \mathcal{O}_{p^e}$ is a prime ideal in \mathcal{O}_{p^e} . This shows that, $p\mathbf{Z}$ is totally ramified with the prime ideal $\langle \zeta - 1 \rangle$ lying above it. Since the discriminant of \mathcal{O}_{p^e} is $\pm p^{p^e-1(p^e-e-1)}$ (see [16], Lemma 10.1), we have p is the only ramified prime in \mathcal{O}_{p^e} and so no other prime of \mathbf{Q} has this property i.e. K_{p^e} is unramified at all primes different from p .

To determine where K_n is ramified, we write out the prime decomposition of $n = p_1^{e_1} \cdots p_t^{e_t}$ over \mathbf{Q} . We require that n is not twice an odd integer, i.e. $n \neq 2n_0$ where n_0 is odd. Then, K_n is the compositum of fields i.e. $K_n = K_{p_1^{e_1}} \vee \cdots \vee K_{p_t^{e_t}}$. It follows that all the primes p_i (that appear in the prime factorisation of n) ramify in K_n and the rest are unramified.

Remark 1.4.2. *The above statement is true over \mathbf{Q} because $\Phi_n(X)$ is irreducible over \mathbf{Q} (for $n \geq 3$) but in general, it is false because $\Phi_n(X)$ may be reducible over some finite fields. In fact, in algebraic number theory, we show that the way $\Phi_n(X)$ factors in $\mathbf{Z}/p\mathbf{Z}$ determines how the ideal $p\mathcal{O}_n$ factors in \mathcal{O}_n . Provided p does not divide the conductor of \mathcal{O}_n (that is for finitely many primes), the factorisation of $\Phi_n(X)$ in $\mathbf{Z}/p\mathbf{Z}$ determines explicitly, the prime ideals that lie above $p\mathbf{Z}$.*

We summarise this argument as follows.

Theorem 1.4.3 (The cyclotomic reciprocity law). *Let $n > 0$ be a positive odd number, ζ_n a primitive n^{th} root of unity, $K_n = \mathbf{Q}(\zeta_n)$. Then K_n/\mathbf{Q} is an abelian extension of degree $\phi(n)$ and $\text{Gal}(K_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*$. A rational prime p is ramified in K_n if and only if p divides n . If $p \nmid n$, the Artin automorphism corresponding to the prime ideal $p\mathbf{Z}$ maps ζ_n to ζ_n^p . If f is the order of p modulo n , then $p\mathbf{Z}$ splits into $\frac{\phi(n)}{f}$ primes each of extension degree f in K_n . Moreover, $\mathcal{O}_n = \mathbf{Z}[\zeta_n]$.*

Proof. ([18], Theorem 12.10). □

Let us mention about the behaviour of the prime or the place at infinity. In \mathbf{Q} , there is only one archimedean prime given by the archimedean absolute value. For $n > 2$, then K_n is such that, every embedding of it into \mathbf{C} is complex. This is because, the only roots of unity that belong to \mathbf{R} are ± 1 . If we consider the $K_n^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real subfield of K_n , then K_n^+ is real and so is every embedding of it into \mathbf{C} . Moreover, $[K_n : K_n^+] = 2$ since $X^2 - (\zeta_n + \zeta_n^{-1})X + 1 \in K_n^+[X]$ is the minimum polynomial of ζ_n over K_n^+ , that is $\text{Gal}(K_n/K_n^+) \cong \mathbf{Z}^* = \{\pm 1\}$. Thus, the prime at infinity splits into $\frac{\phi(n)}{2}$ real primes in K_n^+ and each of these ramifies to a complex prime in K_n . It is clear that $\text{Gal}(K_n/K_n^+) = \langle \sigma_{-1} \rangle$. Therefore, σ_{-1} can be thought of as generating an inertia group for primes at infinity.

Chapter 2

Arithmetic of polynomials over \mathbf{F}_r

The polynomial ring A over finite field \mathbf{F}_r has many important properties associated with the development of algebraic function field theory (or the theory of algebraic curves over a finite field). In this chapter, we shall explore these properties and illustrate how they are analogous to those in \mathbf{Z} . This is the basis of the study of number theory in function fields. Most of the material in this section can be found in the first chapter of Rosen's text [18].

2.1 Polynomials and finite fields

Let \mathbf{F}_r be a finite field with r elements and $\text{Char}(\mathbf{F}_r) = p > 0$, a prime number. So the finite field \mathbf{F}_p (isomorphic to $\mathbf{Z}/p\mathbf{Z}$) is its prime sub field ($\mathbf{F}_p \hookrightarrow \mathbf{F}_r$, with p elements). In general, the number of elements in a finite field is a power of its characteristic. In this case, $r = p^l$, where l is the degree of \mathbf{F}_r considered as an \mathbf{F}_p -extension field (or \mathbf{F}_p -vector space). Now, A is the ring of polynomials in the indeterminate T and coefficients in \mathbf{F}_r .

Every element in A is the form $f := f(T) = \alpha_n T^n + \alpha_{n-1} T^{n-1} + \cdots + \alpha_0$, $n \in \mathbf{N}$. If $\alpha_n \neq 0$, we say f has degree n and we write $\deg(f) = n$. Moreover, $\deg : A \rightarrow \mathbf{Z} \cup \{\infty\}$ defines a non-archimedean valuation on A (see chapter 4). The sign of f , usually denoted by $\text{sgn}(f)$, is α_n . We set the sign of the zero polynomial to be 0 and its degree to be $-\infty$. If the sign of f is $+1$, then $f(T)$ is called a monic (or positive) polynomial. These monics play the role of positive integers in A . We shall denote the set of all monics in A by A^+ .

2.2 Some properties of A

We now have the basic terminology to state and prove the properties of the ring A .

Proposition 2.2.1. $A := \mathbf{F}_r[T]$ is an integral domain.

Proof. Suppose $f(T) = \sum_{i=0}^m \alpha_i T^i$, $g(T) = \sum_{i=0}^n \beta_i T^i$ and $f(T)g(T) = 0$ where $\alpha_i, \beta_i \in \mathbf{F}_r$, then $h(T) = f(T)g(T) = \sum_{k=0}^{m+n} \lambda_k T^k$ has $\lambda_k = 0$, for each k . But $\lambda_k = \sum_{i=0}^k \alpha_{k-i} \beta_i$ for each k . We have $\lambda_0 = \alpha_0 \beta_0$ implying either $\alpha_0 = 0$ or $\beta_0 = 0$. Now suppose $\alpha_0 \neq 0$, (in which case $f \neq 0$), then $\beta_0 = 0$, therefore $\lambda_1 = \alpha_1 \beta_0 + \alpha_0 \beta_1 = 0$ implying $\beta_1 = 0$. Doing this for $i = 2, \dots, m+n$, we obtain $\beta_i = 0$ for all i , therefore $g(T) = 0$. \square

Now that A is an integral domain, we can construct its field of quotients k , the field of rational functions in T over \mathbf{F}_r . Arithmetically, we take this to be analogous to \mathbf{Q} .

Proposition 2.2.2 (Division algorithm). *Let $f, g \in A$, with $g \neq 0$, then there exists $q, r \in A$ such that $f = qg + r$ and $\deg(r) < \deg(g)$. Moreover q, r are uniquely determined.*

Proof. We prove this in two parts as follows.

1. **Existence:** Let $\deg(f) = m$, $\deg(g) = n$, $\text{sgn}(f) = \alpha$, $\text{sgn}(g) = \beta$. By an induction on m ; if $m < n$, set $q = 0$ and $r = f$. If $m \geq n$, we note that $f_1 = f - \alpha\beta^{-1}T^{m-n}g$ has smaller degree than $\deg(f)$. By induction, there exists $q_1, r_1 \in A$ such that $f_1 = q_1g + r_1$ with $\deg(r_1) < \deg(g)$. In this case, set $q = \alpha\beta^{-1}T^{m-n} + q_1$ and $r = r_1$.
2. **Uniqueness:** Let $f = qg + r = q'g + r'$, $q, r, q', r' \in A$ and $\deg(r), \deg(r') < \deg(g)$. Then $(q - q')g = r' - r$ implies g divides $r - r'$, so $r - r' = 0$ hence $q = q'$. Otherwise, we would have $\deg((q - q')g) \geq \deg(g)$ whenever $q \neq q'$ and $\deg(r' - r) < \deg(g)$ whenever $r \neq r'$. Therefore, $(q - q')g = r' - r$ cannot hold unless $q = q'$ and $r = r'$.

Hence existence and uniqueness are established. \square

A is an integral domain endowed with a division algorithm. In particular, A is Euclidean, therefore a principal ideal domain (PID) and consequently a unique factorisation domain (UFD). This also allows a quick proof of the finiteness of the residue class rings.

Theorem 2.2.3. *Suppose $0 \neq g \in A$, then A/gA is a finite ring with $r^{\deg(g)}$ elements.*

Proof. Let $\deg(g) = n$, by theorem (2.2.2), $A_g = \{a \in A : \deg(a) < n\}$ is a complete set of representatives for A/gA . Its elements are of the form $a = \alpha_{n-1}T^{n-1} + \alpha_{n-2}T^{n-2} + \dots + \alpha_0$. Since the coefficients vary independently via \mathbf{F}_r , there are r^n possible such polynomials. \square

It is this theorem that motivates the definition below.

Definition 2.2.4. *Let g be a non-zero polynomial in A , the order of A/gA is $\#(A/gA)$. It is denoted and defined as $|g| = r^{\deg(g)}$. It is also known as a “measure” of size of g .*

If $g = 0$, then $|g| = 0$. We will later prove that in fact, the measure of g is analogous to the absolute value of an integer n , the number of elements in $\mathbf{Z}/n\mathbf{Z}$. Its immediate properties are those of an absolute value function. This is discussed in detail in chapter 4.

To understand the structure of A , we need to first know the structure of A^* , its group of units. Suppose g is a unit in A , by the definition of a unit, there exists $f \in A$, such that $fg = 1$, that is to say, a constant polynomial in A . So $\deg(fg) = \deg(f) + \deg(g) = \deg(1) = 0$ hence $\deg(f) = \deg(g) = 0$. Therefore, the only units in A are the non-zero constant polynomials. This means that, each such a non-zero constant in \mathbf{F}_r is a unit in A (in particular, all units of A belong to \mathbf{F}_r). This explains why we sometimes denote A^* by \mathbf{F}_r^* . Since every non-zero integer can be made positive after multiplication by a suitable $\alpha \in \mathbf{Z}^*$, so can every non-zero polynomial in A be made monic by multiplication with a suitable element $\alpha \in \mathbf{F}_r^*$. In particular, since every finite subgroup of the multiplicative group of a field is cyclic, \mathbf{F}_r^* is a finite cyclic group with $r - 1$ elements and so is A^* (compare this with $\mathbf{Z}^* = \{\pm 1\}$).

A non-constant polynomial f in A is said to be, (i) irreducible if whenever $f = gh$, then either g or h is a constant polynomial i.e. if it cannot be written as a product of two polynomials each of positive degree. (ii) prime if whenever f divides hg , then either f divides h or f divides g , where $h, g \in A$. In every PID, the notion of irreducibility and primeness are equivalent up to units in the domain. Through out this thesis, we work in A , so the terms irreducible and prime will be used interchangeably. By the above definitions, every prime polynomial must be monic. Therefore, we shall characterise a prime P as any monic irreducible polynomial in A . This is analogous to prime numbers $p \in \mathbf{Z}^+$.

Every non-zero polynomial can be written as a product of non-zero constant and a monic polynomial. Therefore, every ideal in A has a unique monic generator which also belongs to A . Since A is a UFD, every non-zero polynomial $f \in A$ can be written uniquely as

$$f = \alpha \prod_{i=1}^t P_i^{e_i}, \quad (2.1)$$

where $\alpha \in \mathbf{F}_r^*$, P_i are distinct monic irreducible polynomials i.e primes, and $e_i \in \mathbf{Z}_{\geq 0}$. This is the analogue of the celebrated fundamental theorem of arithmetic in \mathbf{Z} that states; every $n \in \mathbf{Z}$ can be written as a product of primes in \mathbf{Z} and the factorisation is unique up to order and number of units in \mathbf{Z} . Note, this is true because A is a UFD, otherwise it is false (In Dedekind domains, it can be restored via using prime ideals). This is one of the topics in algebraic number theory, where we try to recover unique factorisation in different rings.

Given $f \in A$, we can investigate the structure of A/fA and its group of units $(A/fA)^*$. To do this we shall need the polynomial version of the chinese remainder theorem.

Theorem 2.2.5 (The chinese remainder theorem). *Let m_1, m_2, \dots, m_t be elements of A that are*

pairwise co-prime and $m = m_1 m_2 \dots m_t$ then

$$(i) \quad (A/mA) \cong (A/m_1A) \times \dots \times (A/m_tA)$$

$$(ii) \quad (A/mA)^* \cong (A/m_1A)^* \times \dots \times (A/m_tA)^*.$$

Let f be non-zero and non-unit, with the prime decomposition as in equation (2.1), then

$$(A/fA)^* \cong (A/P_1^{e_1}A)^* \times \dots \times (A/P_t^{e_t}A)^*.$$

By the above isomorphism, it suffices to determine the structure of the groups $(A/P^eA)^*$.

Proposition 2.2.6. *Let $n \in \mathbf{N}$ and p be prime in \mathbf{Z} ,*

$$(\mathbf{Z}/p^n\mathbf{Z})^* \cong \begin{cases} C_{p^{n-1}(p-1)}, & \text{if } p \text{ is an odd prime,} \\ C_2 \times C_{2^{n-2}}, & \text{if } p = 2 \text{ and } n \geq 3, \\ C_n, & \text{if } p = 2 \text{ and } n \leq 2. \end{cases}$$

Proposition 2.2.7. *Let $0 \neq P \in A$, be a prime, then $(A/PA)^*$ is cyclic of order $|P| - 1$.*

Proof. Since A is a PID, P a prime, we have that PA is a maximal ideal, so A/PA is a field. In particular, we have $(A/PA)^*$ cyclic. The order of this group is clearly $|P| - 1$. \square

However, the situation in $(A/P^eA)^*$ is quite different as shown in proposition 2.2.8.

Proposition 2.2.8. *Let P , be a prime and $e \in \mathbf{N}$, the order of $(A/P^eA)^*$ is $|P|^{e-1}(|P| - 1)$. The kernel of the canonical map $\theta : (A/P^eA)^* \rightarrow (A/PA)^*$ is a p -group of order $|P|^{e-1}$. As $e \rightarrow \infty$, the minimal number of generators in the kernel tends to infinity.*

Proof. ([18], Proposition 1.6). \square

The structure of these groups gets very complicated and surely does cause problems in the more advanced parts of the theory. This is one of the many sources of non-analogies that exist between \mathbf{Z} and A . In general, it looks like the analogy between \mathbf{Z} and A breaks down, however we will recover this good analogy by using the Carlitz module (see chapters 4, 5).

2.3 Euler's and Fermat's little theorems

Let A_f be the set of representatives of A/fA given by $A_f = \{a \in A : 0 \leq \deg(a) < \deg(f)\}$. Since $1 \in A_f$ is a unit, by standard theory of associates, every non-zero polynomial a is a unit in A_f if and only if $(a, f) = 1$, therefore we can also define

$$(A/fA)^* = \{a \in A : \deg(a) < \deg(f) \text{ and } (a, f) = 1\}.$$

Definition 2.3.1 (Euler-totient function). *Let $f \in A$ be a non-zero polynomial, the number of elements in the group $(A/fA)^*$ is $\varphi(f)$.*

This is the polynomial version of the Euler-totient function. Its analogous properties such as multiplicativity follows from counting principles. Having defined the Euler-totient function, it is always natural to state the analogue of Euler's and Fermat's little theorems.

Proposition 2.3.2 (Euler's theorem). *If $f \in A$ is a non-zero polynomial and $a \in A$ is such that $(a, f) = 1$, then $a^{\varphi(f)} \equiv 1 \pmod{f}$.*

Proof. $\#(A/fA)^* = \varphi(f)$. By standard group theory (Lagrange's theorem), $\bar{a}^{\varphi(f)} = 1$ for all $a \in (A/fA)^*$. If $(a, f) = 1$, then $\bar{a} = a + fA \in (A/fA)^*$ and so $a^{\varphi(f)} \equiv 1 \pmod{f}$. \square

Corollary 2.3.3 (Fermat's little theorem). *If $P \in A$ is a prime and $a \in A$ is relatively prime to P , then $a^{|P|-1} \equiv 1 \pmod{P}$.*

Proof. Since P is irreducible, we have $(a, P) = 1$ if and only if $P \nmid a$. The corollary follows from proposition 2.3.2 and the fact that, for an irreducible P , $\phi(P) = |P| - 1$. \square

Like in elementary number theory, the theorems above play an important role in the study of arithmetic of function fields, for example in the proof of the Wilson's theorem as illustrated later, and more pertinent, in our study of cyclotomic polynomials and extensions.

Proposition 2.3.4. *Let $P \in A$ be a prime of degree n , X an indeterminate, then*

$$X^{|P|-1} - 1 \equiv \prod_{0 \leq \deg(f) < n} (X - f) \pmod{P}.$$

Proof. ([18], Proposition 1.9) Since P is irreducible over k , (A/PA) is a field, therefore $(A/PA)^*$ has order $|P| - 1$. Recall, $A_P = \{f \in A : \deg(f) < n\}$ is a set of representatives of the cosets of A/PA . If we remove $f = 0$, we get the set of representatives for $(A/PA)^*$. We find,

$$X^{|P|-1} - 1 \equiv \prod_{0 \leq \deg(f) < n} (X - \bar{f}) \pmod{P}, \quad (2.2)$$

where the bars denote cosets modulo P . This follows from proposition (2.3.3) and the fact both sides of the equation are monic polynomials in X with the same roots in the field A/PA . Since there are exactly $|P| - 1$ roots on both sides and the difference between the two sides has degree less than $|P| - 1$, this difference must be identically 0. The congruence in proposition 2.3.4 is equivalent to this assertion. \square

Corollary 2.3.5 (Wilson's theorem).

$$\prod_{0 \leq \deg(f) < n} f \equiv -1 \pmod{P}. \quad (2.3)$$

Proof. In proposition (2.3.4), set $X = 0$.

If the characteristic of \mathbf{F}_r is 2, then the result follows since $-1 \equiv 1 \pmod{2}$. Otherwise i.e when the characteristic of \mathbf{F}_r is odd, then $|P| - 1$ is even and still the result follows. \square

It is interesting to note that in the polynomial version of Wilson’s theorem, the LHS of the congruence depends on the degree of the P (the valuation of P) and not on P itself.

Definition 2.3.6. *The zeta function of A , denoted $\zeta_A(s)$, is defined by the infinite series*

$$\zeta_A(s) := \sum_{f \in A^+} \frac{1}{|f|^s}. \tag{2.4}$$

Evidently, since the number of monic polynomials of fixed degree n is r^n , we have

$$\zeta_A(s) := \sum_{f \in A^+} \frac{1}{|f|^s} = \sum_{n=0}^{\infty} \frac{r^n}{r^{ns}} = \frac{1}{1 - r^{1-s}}, \tag{2.5}$$

convergent for $\Re(s) > 1$. Unlike in the classical Riemann-zeta function (whose analytic continuation is much harder to establish), the analytic continuation of $\zeta_A(s)$ to a meromorphic function over \mathbf{C} is obvious from the relation $\zeta_A(s) = (1 - r^{1-s})^{-1}$. Now, $\zeta_A(s)$ has a simple pole at $s = 1$, with a residue of $\frac{1}{\log(r)}$. In fact, it also satisfies a simple functional equation. Its other properties are relatively easy to prove unlike for the classical zeta function. Similar statements hold for the generalisations of the zeta function in the context of function fields over finite field, however, their proofs are more difficult to establish [18]. Since A is a factorial, (by the unique factorisation theorem), we have

$$\begin{aligned} \zeta_A(s) &= \sum_{f \in A^+} \frac{1}{|f|^s} = \prod_P \left\{ 1 + \frac{1}{|P|^s} + \frac{1}{|P|^{2s}} + \dots \right\} \\ &= \prod_P \left\{ 1 - \frac{1}{|P|^s} \right\}^{-1} = \prod_{n=1}^{\infty} \left\{ 1 - \frac{1}{r^{ns}} \right\}^{-v(n)} \end{aligned} \tag{2.6}$$

where $v(n)$ denotes the number of primes of degree n . Comparing (2.4),(2.6), we get

$$1 - r^{1-s} = \prod_{n=1}^{\infty} \{1 - r^{-ns}\}^{v(n)}. \tag{2.7}$$

We define the Möbius function for polynomials as,

$$\mu(f) = \begin{cases} (-1)^s, & f \text{ is square free with } s \text{ distinct prime factors,} \\ 0, & f \text{ has a square factor.} \end{cases}$$

Moreover,

$$\sum_{f \in A^+, \deg(f)=n} \mu(f) = \begin{cases} 1, & n = 0 \\ -r, & n = 1 \\ 0, & n > 1. \end{cases}$$

Sketch proof. It is trivial for $n = 0$. Suppose $n \geq 1$, then

$$\sum_{m \in A^+} \frac{\mu(f)}{|f|^s} = \prod_P \left\{ 1 - \frac{1}{|P|^s} \right\} = \frac{1}{\zeta_A(s)} = 1 - r^{1-s}.$$

Clearly, $\sum_{\deg(f)=0} \mu(f) = 1$, $\sum_{\deg(f)=1} \mu(f) = -r$ and $\sum_{\deg(f)=n} \mu(f) = 0$ for $n \geq 2$. \square

An arithmetic function is a real or complex valued function f defined on A^+ . e.g. the Möbius μ , the Euler totient function ϕ e.t.c. We define the unit function u to be the arithmetic function such that $u(f) = 1$ for all $f \in A^+$. The identity function \mathcal{I} is defined as $\mathcal{I}(1) = 1$ and $\mathcal{I}(f) = 0$ for all $f \in A^+$. One can show that $\sum_{d|f} \mu(d) = \mathcal{I}(f)$. Recall, if f, g are arithmetical functions on A , we define their Dirichlet product $f * g$ to be the to be the arithmetical function h defined by $h(a) = \sum_{d|a} f(d)g(\frac{a}{d})$ for any $a \in A^+$. So we can rewrite $\sum_{d|f} \mu(d) = \mathcal{I}(f)$ as $\mu * u = \mathcal{I}$. So μ and u are Dirichlet inverses of each other.

Proposition 2.3.7 (Möbius inversion formula). *Suppose $f \in A$ and \mathcal{F}, \mathcal{G} are (function field) arithmetic functions, then*

$$\begin{aligned} \mathcal{F}(f) &= \sum_{d|f} \mathcal{G}(d) \\ &\text{if and only if,} \\ \mathcal{G}(f) &= \sum_{d|f} \mathcal{F}(d) \mu\left(\frac{f}{d}\right). \end{aligned}$$

Proof. From above we have $\mathcal{F} = \mathcal{G} * u$ so multiplication by μ gives $\mathcal{F} * \mu = (\mathcal{G} * u) * \mu = \mathcal{G}$. Conversely, the Dirichlet product of $\mathcal{F} * \mu$ by u gives $\mathcal{F} = (\mathcal{F} * \mu) * u = \mathcal{G} * u$. \square

Proposition 2.3.8. *For any $0 \neq f \in A$, we have*

$$|f| = \sum_{d|f} \varphi(d).$$

Corollary 2.3.9.

$$\varphi(f) = \sum_{d|f} \mu(d) \left| \frac{f}{d} \right|.$$

Taking the logarithmic derivative with respect to r on both sides of equation 2.7 and multiplying the result by r^{-s} yields

$$\frac{r^{1-s}}{1-r^{1-s}} = \sum_{n=1}^{\infty} \frac{nv(n)r^{-n}}{1-r^{-ns}}.$$

Finally, expanding both sides into power series using the geometric series and compare coefficients of r^{-ns} . The result is the beautiful formula, (often attributed to R. Dedekind)

$$r^n = \sum_{d|n} dv(d)$$

and by the Möbius inversion we obtain,

Corollary 2.3.10.

$$v(n) = \frac{1}{n} \sum_{d|n} \mu(d)r^{\frac{n}{d}}.$$

Chapter 3

Additive polynomials

In this chapter, we will discuss the theory of additive polynomials and the algebraic structure carried by their roots. This chapter should be read independently of all the others in order to appreciate it. The notation in it is local to itself, so should not be confused with that of chapters 2 and the rest. It aims at stating results that will be assumed later on in chapters 4 and 5 without proof. We will closely follow chapter 2 of [10] omitting some details.

3.1 Basic properties of additive polynomials

Let \mathcal{F} be a finite field of characteristic p , and $\bar{\mathcal{F}}$ be its fixed algebraic closure. A polynomial $f(X) \in \mathcal{F}[X]$ is said to be additive if inside $\mathcal{F}[X, Y]$, a polynomial ring in two variables X and Y , we have $f(X + Y) = f(X) + f(Y)$. We say $f(X)$ is absolutely additive if and only if $f(X)$ is additive over the fixed algebraic closure of \mathcal{F} . We illustrate this below.

1. The p^{th} -power map $\tau(X) = X^p$ is absolutely additive for any \mathcal{F} . This follows trivially from the fact that $(X + Y)^p = X^p + Y^p$ in any field of characteristic p .
2. For any $\alpha \in \mathcal{F}$, with $f(X) = \alpha X$, the homogeneous linear polynomial is additive. In characteristic zero fields, this collection constitutes the set of all additive polynomials.

One can check with ease that the following lemma is true for additive polynomials.

Lemma 3.1.1. *Let $\alpha \in \mathcal{F}$ and $f(X), g(X)$ be additive polynomials, then $(f + g)(X), \alpha f(X)$ and $g(f(X))$ are all additive polynomials.*

From lemma 3.1.1, it follows that the monomials $\tau_p^i(X) = X^{p^i}$, as well their linear span (that is, the polynomials of the form $f(X) = \sum_{i=0}^n \alpha_i X^{p^i}$, where $\alpha_i \in \mathcal{F}$) are absolutely additive.

The set of all additive polynomials in $\mathcal{F}[X]$ is denoted by $\mathcal{F}\{\tau_p\}$. It is a straight forward exercise to show that actually $\mathcal{F}\{\tau_p\}$ forms a ring under usual addition and the multiplication defined by composition of functions (not ordinary multiplication). We denote this ring by $\mathcal{F}\{\tau_p\}$ and call it, the *twisted polynomial ring*. Some texts denote $\mathcal{F}\{\tau_p\}$ by $\mathcal{A}(\mathcal{F})$. If we view $\mathcal{F}[X]$ as a vector-space of polynomials in indeterminate X , then $\mathcal{F}\{\tau_p\}$ is a subspace of $\mathcal{F}[X]$. $\mathcal{F}\{\tau_p\}$ is sometimes referred to as the ring of Frobenius polynomials or p -polynomials.

Theorem 3.1.2. *Let E be an infinite field of characteristic p , then $f(X) \in E[X]$ is additive if and only if $f(X) \in E\{\tau_p\}$.*

Proof. ([10], Theorem 1.1.5). □

Proposition 3.1.2 is false if E is a finite field, e.g. for $f(x) = x + (x^3 - x)^2 \in \mathbf{F}_3[x]$, we have, $f(x)$ is additive but does not belong to $\mathbf{F}_3\{\tau_3\}$, since $f(x) = x + (x^3 - x)^2 = x^6 + x^4 + x^2 + x$.

Corollary 3.1.3. *The set of all absolutely additive polynomials over \mathcal{F} is $\mathcal{F}\{\tau_p\}$.*

Proof. The algebraic closure of any field is infinite, so we can apply proposition 3.1.2. □

From now onwards, we shall drop the term ‘absolutely’ and adopt the adjective additive to refer to an element of $\mathcal{F}\{\tau_p\}$. We fix the p^{th} power, $r = p^l$ where $l \in \mathbf{N}$. Further, assume $\mathbf{F}_r \subseteq \mathcal{F}$ in order to look for additive polynomials which commute with elements of \mathbf{F}_r . We set $\tau := \tau_p^l$ and let $\mathcal{F}\{\tau\}$ be the composition ring of polynomials in the indeterminate τ . In this case, the ring $\mathcal{F}\{\tau\}$ forms an \mathbf{F}_r -algebra of \mathbf{F}_r -linear polynomials.

It is not true that $f \in \mathcal{F}\{\tau\}$ is obtained from $f(X)$ by formally substituting τ for X , but by via the power map $\tau(X) = X^r$. Indeed $\tau\alpha = \alpha^r\tau$ where $\alpha \in \mathcal{F}$. In general, if $\mathcal{F} \neq \mathbf{F}_p$, then $\mathcal{F}\{\tau\}$ is a non-commutative ring. However, for $\mathbf{F}_r \subseteq \mathcal{F}$, we have commutation since $\alpha^r = \alpha$ for all $\alpha \in \mathbf{F}_r$. We reformulate the structure of $\mathcal{A}(\mathcal{F})$ in a more convenient way through associating to every additive polynomial $f(X) \in \mathcal{A}(\mathcal{F})$, a polynomial $f \in \mathcal{F}\{\tau\}$ using $\tau(X) = X^r$. This sets up a bijection between $\mathcal{A}(\mathcal{F})$, and $\mathcal{F}\{\tau\}$ defined by $f(X) := f(\tau)(X)$.

In a similar manner, we say $f \in \mathcal{F}\{\tau\}$ is monic if and only if $f(X)$ is monic. Consider $f = \alpha_0 + \alpha_1\tau + \dots + \alpha_s\tau^s$, $\alpha_s \neq 0$, we set $s = \deg(f)$ and note that $r^s = \deg(f(X))$. In other words, $\mathcal{F}\{\tau\}$ is similar to $\mathcal{F}[X]$ except that the multiplication of τ by elements of k is given by the mapping $\tau(X) = X^r$ or generally $f(X) = f(\tau)(X)$. In summary, $\mathcal{F}\{\tau\}$ has usual commutative ring operations such that $\tau(\alpha X) = \alpha X^r \tau$ for all $\alpha \in \mathbf{F}_r \subseteq \mathcal{F}$.

3.2 Classification of additive polynomials

If $f \in \mathcal{F}\{\tau\}$, then the roots of f form an \mathbf{F}_r -submodule of \mathcal{F} . If in addition, $f(X)$ is separable, the converse is also true hence the “fundamental theorem of additive polynomials”.

Theorem 3.2.1 (Fundamental theorem of additive polynomials). *Let $f(X) \in \mathcal{F}[X]$ be separable, $W = \{w \in \mathcal{F} : f(w) = 0\}$. Then $f(X)$ is additive if and only if W is a subgroup.*

Proof. ([10], Theorem 1.2.1) (\Rightarrow) Trivial.

(\Leftarrow) Let W be an additive subgroup of \mathcal{F} and

$$f(X) = f_W(X) = \prod_{w \in W} (X - w), \quad \text{i.e. separable.}$$

We are required to show that $f(X)$ is additive. In particular, $f(X + w) = f(X)$ for $w \in W$.

Now if we let $y \in \mathcal{F}$ and $h(X) = f(X + y) - f(X) - f(y)$. Clearly $\deg(h) < \deg(f)$. On the other hand, $h(w) = f(w + y) - f(w) - f(y) = f(w + y) - f(y)$ for $w \in W$ and any $y \in \mathcal{F}$. This implies $h(w) = 0$, and as $n = \deg(f) > \deg(h)$, we conclude that $h(X) \equiv 0$. Now let Y be an indeterminate and $h_1(X) = f(X + Y) - f(X) - f(Y) \in \mathcal{F}[Y][X] = \mathcal{F}[X, Y]$. We conclude $h_1(\alpha) = 0$ for $\alpha \in \mathcal{F}$. As \mathcal{F} is infinite, $h_1(Y) \equiv 0$ and thus, $f(X)$ is additive. \square

Corollary 3.2.2. *Suppose $f(X) \in \mathcal{F}[X]$ is separable, then $f(X)$ is \mathbf{F}_r -linear if and only if its roots form an \mathbf{F}_r -subspace.*

Proof. ([10], Corollary 1.2.2) It is clear that if $f(X) \in \mathcal{F}[X]$ is \mathbf{F}_r -linear then W , the set of roots of $f(X)$ is indeed an \mathbf{F}_r -subspace. So we only need to show that if W is an \mathbf{F}_r -vector subspace of k , then $f(X)$ is \mathbf{F}_r -linear. Let $h(X) = f(\alpha X) - \alpha f(X)$ where $\alpha \in \mathbf{F}_r$. The cardinality of W is $|W| = r^s$ for some $s \in \mathbf{N}$, and so $\deg(f) = r^s$. Assume the leading term of $f(X)$ is cX^{r^s} , and so $h(X) = f(\alpha X) - \alpha f(X) = c(\alpha X)^{r^s} + \dots - (\alpha cX^{r^s} + \dots) =$ terms of degree $< r^s$, since $\alpha^{r^s} = \alpha$ for any $\alpha \in \mathbf{F}_r$, and so we conclude that $\deg(h) < r^s$. On the other hand, $h(w) = 0$, $w \in W$, therefore $h(X)$ must identically vanish, therefore $f(\alpha X) = \alpha f(X)$. \square

Having introduced the notion of a vector-space on the roots of additive polynomials, all standard results from linear algebra follow suit. Later, we shall see that; for some particular polynomials f , the set of its roots is more than a vector space; we can define an A -module structure on them. In addition, consider $W \subseteq \mathcal{F}$, an \mathbf{F}_r -subspace and $\{w_1, \dots, w_n\} \subseteq W$.

Definition 3.2.3. *Let*

(a) We define the Moore determinant $\Delta(w_1, \dots, w_n) := \Delta_r(w_1, \dots, w_n)$ as,

$$\Delta_r(w_1, \dots, w_n) = \det \begin{pmatrix} w_1 & w_2 & \dots & w_n \\ w_1^r & w_2^r & \dots & w_n^r \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{r^{n-1}} & w_2^{r^{n-1}} & \dots & w_n^{r^{n-1}} \end{pmatrix}.$$

Lemma 3.2.4. $\{w_1, \dots, w_n\} \subset \mathcal{F}$ is \mathbf{F}_r -linearly independent if and only if $\Delta(w_1, \dots, w_n) \neq 0$.

Proof. ([10], Proposition 1.3.3). □

So, if $\text{Dim}_{\mathbf{F}_r}(W) = n$, then $\{w_1, \dots, w_n\}$ is an \mathbf{F}_r -basis for W if and only if $\Delta(w_1, \dots, w_n) \neq 0$.

We have so far characterised separable \mathbf{F}_r -linear polynomials as those separable polynomials whose roots form a finite dimensional \mathbf{F}_r -vector space. Using the Moore determinant, one can now be a bit more specific about this subspace W and its associated \mathbf{F}_r -linear polynomial. In some way, this polynomial encodes information about the vector-space.

Let $W \subseteq \mathcal{F}$ be a finite dimensional \mathbf{F}_r -vector-space, $\{w_1, \dots, w_n\}$ be a chosen \mathbf{F}_r -basis for W and for $1 \leq i \leq n$, let W_i be the linear span of $\{w_1, \dots, w_i\}$. We set

$$f_i(X) := f_{W_i}(X) = \prod_{\alpha \in W_i} (X - \alpha) = \frac{\Delta_i(X)}{\Delta_{i-1}(w_i)},$$

where $\Delta_i(X) = \Delta(w_1, \dots, w_i, X)$ and $\Delta_{i-1}(w_i) = \Delta(w_1, \dots, w_i)$.

By construction, $\Delta_i(X) = 0$ if and only if $X \in W_i$ (follows from column operations). This implies that $\Delta_i(X) = c_i \prod_{\alpha \in W_i} (X - \alpha)$ with $\deg(\Delta_i(X)) = \#W_i = r^i$. In particular, we have $\Delta_n(X) = c_n f_n(X)$, where $c_n = \Delta_{n-1}(w_n)$, is the leading coefficient of $\Delta_n(X)$. This is actually the determinant of the cofactor matrix of the nn -entry in the corresponding Moore matrix. This is obtained by deleting the n^{th} row and the n^{th} column from the Moore matrix.

If \mathcal{F} is Galois over some field \mathcal{F}_1 and for some i , both W_i and W are $\text{Gal}(\mathcal{F}/\mathcal{F}_1)$ stable, then $f_W, f_i, f_{\bar{W}_i}$ all belong to $\mathcal{F}_1\{\tau\}$, where \bar{W}_i is the linear-span of $f_i(w_{i+1}), \dots, f_i(w_n)$.

3.3 Properties of the rings $\mathcal{F}[X]$ and $\mathcal{F}\{\tau\}$

In this section, we highlight some of the properties of $\mathcal{F}\{\tau\}$ in a more concrete way in relation to those of $\mathcal{F}[X]$. We begin by remarking that since \mathcal{F} is a field, $\mathcal{F}\{\tau\}$ is an integral domain. This implies, multiplication in $\mathcal{F}\{\tau\}$ permits both, left and right hand cancellation even-though they are not necessarily the same. This section attempts to make the two rings

familiar, as work with both in chapter 5 and also to capture some important results that are adopted/assumed while studying Carlitz cyclotomic extensions.

Proposition 3.3.1. *If $f(X) \in \mathcal{F}[X]$, then there exists $g \in \mathcal{F}\{\tau\}$ such that $f(X)$ divides $g(X)$.*

Proof. Let $\bar{\mathcal{F}}$ be a fixed algebraic closure of \mathcal{F} and $\{w_1, \dots, w_n\} \subset \bar{\mathcal{F}}$ be the roots of $f(X)$ chosen without multiplicity. Let $W = \langle w_1, \dots, w_n \rangle$ be the \mathbf{F}_r -linear span of $\{w_1, \dots, w_n\}$ and define $f_W(X) := \prod_{w \in W} (X - w)$. Therefore, $f_W(X)$ is \mathbf{F}_r -linear. If we let t be the largest multiplicity of any w_i and s be the smallest positive integer so that $r^s \geq t$. We now define $g = \tau^s f_W(\tau) \in \mathcal{F}\{\tau\}$, and so we obtain $g(X) = f(X^{r^s}) \in \mathbf{F}_r[X]$, so $f(X)$ divides $g(X)$. \square

This asserts that, every $f(X) \in \mathcal{F}[X]$ is a factor to some $g(X) \in \mathcal{F}\{\tau\}$. In this case, if $\mathbf{F}_r \subseteq \mathcal{F}$, then every Galois extension of \mathcal{F} is a splitting field for some \mathbf{F}_r -linear polynomial.

In the remaining part of this chapter, we let $f \in \mathcal{F}\{\tau\}$ and $f(X) \in \mathcal{F}[X]$. Multiplication shall be the product in the respective rings i.e. $fg = f \circ g$ and $f(X)g(X) = f(X) \cdot g(X)$. If h is any other polynomial such that $f(X)$ divides $h(X)$, then the \mathbf{F}_r -vector subspace W is contained in the set of roots of $h(X)$, therefore by the preceding arguments, there exists g_1 such that $h = g_1g$. However, since $\mathcal{F}\{\tau\}$ is (in general) non-commutative, the left and right cancellation may not necessarily yield the same remainder. We say, $f \in \mathcal{F}\{\tau\}$ is right divisible by $g \in \mathcal{F}\{\tau\}$ if there exists $h \in \mathcal{F}\{\tau\}$ such that $f = hg$. Similarly, we define $f \in \mathcal{F}\{\tau\}$ to be left divisible by $g \in \mathcal{F}\{\tau\}$ if there exists $h \in \mathcal{F}\{\tau\}$ such that $f = gh$.

Proposition 3.3.2 (Right division). *Let $\{f, g\} \subset \mathcal{F}\{\tau\}$, $g \neq 0$. Then, $\exists h, r \in \mathcal{F}\{\tau\}$, with $\deg(r) < \deg(g)$ such that $f = hg + r$. Moreover h and r are uniquely determined.*

Proof. ([10], Proposition 1.6.2). \square

Every left ideal in $\mathcal{F}\{\tau\}$ is principal, its right division algorithm is similar to that in $\mathcal{F}[X]$.

The analogous proposition for left division is false in general. However, if \mathcal{F} is perfect (for each $x \in \bar{\mathcal{F}}$, there exists $j \geq 0$ such that $x^{p^j} \in \mathcal{F}$) i.e. $\tau(\mathcal{F}) = \mathcal{F}$, then left division is guaranteed. Perfect fields have a property that every finite extension of them is separable. If $\mathcal{F} = \bar{\mathcal{F}}$, then left division follows directly since every algebraically closed field is perfect.

Proposition 3.3.3 (Left division). *Let $f, g \in \bar{\mathcal{F}}\{\tau\}$, $g \neq 0$, then there exists $h, r \in \bar{\mathcal{F}}\{\tau\}$, with $\deg(r) < \deg(g)$ such that $f = gh + r$. Moreover, h, r are uniquely determined.*

Proof. ([10], Proposition 1.6.5). \square

If \mathcal{F} is perfect, then every right ideal in $\mathcal{F}\{\tau\}$ is principal. In the example below, we illustrate that indeed, the two division algorithms are not necessarily the same. However in most of the calculations, we shall work in $\mathcal{F}[\tau]$ with the right hand division algorithm.

Example 3.3.4. We divide f by g where $f = \tau^2 - \tau$, $g = \tau - T\tau^0$ using both algorithms.

1. $\tau^2 - \tau = (\tau + (T^r - 1)\tau^0)(\tau - T\tau^0) + (T(T^r - 1)\tau^0)$ (by right division algorithm).
2. $\tau^2 - \tau = (\tau - T\tau^0)(\tau + (T - 1)^{\frac{1}{r}}\tau^0) + (T(T - 1)^{\frac{1}{r}}\tau^0)$ (by left division algorithm).

For simplicity, we define the greatest common factor (GCD) of f and g as the monic generator of the left ideal generated by both f and g . We denote it by (f, g) . By using the euclidean algorithm, we can compute the GCD of f and g . If $h = (f, g)$ the GCD of f and g , then $h(X) = (f(X), g(X))$ since the right division algorithms for $\mathcal{F}\{\tau\}$ and $\mathcal{F}[X]$ are the same (and so are the remainders). We say f and g are co-prime if $(f, g) = \tau^0$.

Let $f, g \in \mathcal{F}\{\tau\}$, the least common multiple of f and g , $[f, g]$ is the monic polynomial of least degree in $\mathcal{F}\{\tau\}$ that is right divisible by both f and g . By definition, this coincides with the monic generator of the left ideal $\mathcal{I} :=$ the intersection of the left ideals generated by f and g i.e. $\mathcal{I} = \langle f \rangle \cap \langle g \rangle$. By proposition 3.3.2, this ideal exists and is principal.

Example 3.3.5. Let $f = \tau + \tau^0$, $g = \tau$. One can easily show that $[f, g] = \tau^2 + \tau$.

Now, $f(X) = X^r + X$, $g(X) = X^r$, their LCM is $X^{2r-1} + X^r \neq X^{r^2} + X^r = (\tau^2 + \tau)(X)$. The notion of least common multiple of two polynomials differs in $\mathcal{F}[X]$ and $\mathcal{F}\{\tau\}$. If we let $f, g \in \mathcal{F}\{\tau\}$ and $h = [f, g]$. Let $h_0(X)$ be the least common multiple of $f(X)$ and $g(X)$. It is clear that $h_0(X)$ divides $h(X)$. For example, for $f(X), g(X)$ given above, $h_0(X) = X^{2r-1} + X^r$ and $h(X) = X^{r^2} + X^r$. It is also clear that $h_0(X)$ divides $h(X)$ since $r - 1$ divides $r^2 - r$.

Chapter 4

Carlitz module

We shall review the basic background material concerning valuations, global fields and their extensions. Here the term ‘*global field*’ refers to either a number field \mathcal{F} , or the function field \mathcal{F} of an algebraic curve over a finite field, that is to say $\mathcal{F} := \mathcal{F}/k$. While we are later only interested in the latter, much of the theory applies in a unified way to both settings. Good references for this material include ([18], chapter 3), ([19], chapter 2) and ([22], chapter 1).

4.1 Valuation theory

An **ordered group** \mathcal{G} is an abelian group $(\mathcal{G}, +)$ endowed with an order relation \geq in such a way that, the group operation is preserved under the order relation, that is to say, for any $a, b \in \mathcal{G}$, if $a \geq b$, then $(a + c) \geq (b + c)$ for all $c \in \mathcal{G}$. In particular, \mathcal{G} is torsion-free.

Definition 4.1.1. *Let \mathcal{F} be an arbitrary field, \mathcal{G} an ordered group. A valuation v over \mathcal{F} is a surjection $v : \mathcal{F} \rightarrow \mathcal{G} \cup \{\infty\}$ such that for all $x, y \in \mathcal{F}$,*

- (i) $v(x) = \infty$ if and only if $x = 0$.
- (ii) $v(xy) = v(x) + v(y)$.
- (iii) $v(x + y) \geq \min \{v(x), v(y)\}$ and the equality holds if and only if $v(x) = v(y)$.

We call \mathcal{G} , the valuation group of \mathcal{F} . If \mathcal{G} is isomorphic to \mathbf{Z} , then v is a discrete valuation. In this section, we shall develop the theory over an arbitrary field \mathcal{F} , however the results for function fields can be recovered by just replacing \mathcal{F} with the rational function field k .

Define the ring $R_{\mathcal{F}} := \{z \in \mathcal{F} : v(z) \geq 0\}$ and set $\mathfrak{m} := \{z \in \mathcal{F} : v(z) > 0\}$. In this case, the set \mathfrak{m} is an ideal and coincides with the set of all the non-invertible elements of $R_{\mathcal{F}}$. Therefore, $R_{\mathcal{F}}$ is local with \mathfrak{m} as its unique maximal ideal. We call $R_{\mathcal{F}}$, the ring of integers of

\mathcal{F} with respect to the valuation v at the prime \mathfrak{m} . The field $\mathfrak{k} = R_{\mathcal{F}}/\mathfrak{m}$ is called the residue class field (or simply the residue field). The image of an element $\alpha \in R_{\mathcal{F}}$ is denoted by $\bar{\alpha}$ in \mathfrak{k} and is called the residue of α in \mathfrak{k} . Moreover, the set of invertible elements of $R_{\mathcal{F}}$ forms a multiplicative group $R_{\mathcal{F}}^*$, called the units of $R_{\mathcal{F}}$. We summarise this as follows.

Proposition 4.1.2. *Let (\mathcal{F}, v) be a valued field, $R_{\mathcal{F}} = \{z \in \mathcal{F} : v(z) \geq 0\}$ be its valuation ring. $R_{\mathcal{F}}$ is local with the unique maximal ideal $\mathfrak{m} = \{z \in \mathcal{F} : v(z) > 0\}$, where $R_{\mathcal{F}}^* = \{z \in K : v(z) = 0\}$, the group of units. Moreover, the field of fractions of $R_{\mathcal{F}}$ is \mathcal{F} and the value group of \mathcal{F} is $\cong \mathcal{F}^*/R_{\mathcal{F}}^*$.*

Proof. ([19], standard exercise). □

Later, we shall identify each $\mathfrak{m} := \mathfrak{m}_P$ with a prime divisor (or simply prime) of \mathcal{F} and denote it by P , (with abuse of notation); for each prime P in \mathcal{F} , we associate a valuation v_P which gives rise to a valuation ring $R_{\mathcal{F}, \mathfrak{m}}$ with maximal ideal \mathfrak{m} . We denote by $\mathfrak{M}_{\mathcal{F}}$, the set of maximal ideals of all possible $R_{\mathcal{F}}$'s. If \mathcal{F} is a function field and \mathbf{Z} is its value group, then to every prime $P \subset \mathcal{F}$, we associate a prime ideal \mathfrak{m}_P and therefore a discrete valuation $v_P : \mathcal{F} \rightarrow \mathbf{Z} \cup \{\infty\}$, that measures the order of zeroes or poles of a function at P . (a negative valuation implies the function has a pole at P and by convention, $v_P(0) = \infty$).

If the valuation v on field \mathcal{F} is discrete, then $R_{\mathcal{F}}$ is called a discrete valuation ring, (DVR). In this thesis, all our valuations will be discrete. In order to develop the theory concretely, we shall maintain the notation $\mathcal{F}, R_{\mathcal{F}}, \mathfrak{m}$ for the field, its discrete valuation ring (a.k.a. local Dedekind domain) and the corresponding maximal ideal. Any $\pi \in \mathfrak{m}$ is a prime (uniformising) element of the valuation if and only if $v(\pi) = 1$. Now, if $x \in \mathcal{F}^*$ is such that $v(x) = n$, for some $n \in \mathbf{Z}$, then x can be represented uniquely (upto units in \mathcal{F}) as $x = \varepsilon\pi^n$ with $\varepsilon \in R_{\mathcal{F}}^*$. In particular, if $x \in \mathfrak{m}$, then $x = \varepsilon\pi^n$ for some $\varepsilon \in R_{\mathcal{F}}^*$, so $\mathfrak{m} = \langle \pi \rangle$, therefore \mathfrak{m} is a principal ideal. Moreover, every non-zero ideal of $R_{\mathcal{F}}$ is an \mathfrak{m} -power.

Proposition 4.1.3. *Let \mathcal{F} be a discrete valued field, the maximal ideal \mathfrak{m} of the discrete valuation ring $R_{\mathcal{F}}$ is principal and is generated by any prime element $\pi \in \mathcal{R}_{\mathcal{F}}$. Every non-zero ideal of $R_{\mathcal{F}}$ is a power of \mathfrak{m} , and the intersection of all proper ideals of $R_{\mathcal{F}}$ is the zero ideal. Moreover, $\mathcal{F}^* \cong R_{\mathcal{F}}^* \times \mathbf{Z}$.*

Proof. ([19], Theorem 2.2.20).

To prove the last part, let $x \in \mathcal{F}^*$, we can write $x = \varepsilon\pi^n$ in a unique way up-to units in $R_{\mathcal{F}}^*$, and therefore $\lambda : \mathcal{F}^* \rightarrow R_{\mathcal{F}}^* \times \mathbf{Z}$, defined by $\lambda(x) = (\varepsilon, n)$, is the required isomorphism. □

Example 4.1.4. *Consider a number field \mathcal{F} , $\mathcal{O}_{\mathcal{F}}$ its ring of integers and \wp a prime ideal in $\mathcal{O}_{\mathcal{F}}$. Since $\mathcal{O}_{\mathcal{F}}$ is a Dedekind domain, for every $z \in \mathcal{F}^*$, the principal ideal $z\mathcal{O}_{\mathcal{F}}$ in $\mathcal{O}_{\mathcal{F}}$ decomposes as $z\mathcal{O}_{\mathcal{F}} = \wp^n \frac{\mathfrak{a}}{\mathfrak{b}}$, $n \in \mathbf{Z}$ where $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathcal{O}_{\mathcal{F}}$ relatively prime to \wp . We define $v_{\wp}(z) = n$ and take v_{\wp} -as the extension of v_p in \mathcal{F} , (of course $p\mathbf{Z} = \wp \cap \mathbf{Z}$).*

If the value group \mathcal{G} of v is contained in $(\mathbf{R}, +)$, then v induces an absolute value function $|\cdot| : \mathcal{F} \rightarrow \mathbf{R}_{\geq 0}$ by setting $|x|_v = \alpha^{v(x)}$, where $\alpha \in \mathbf{R}$, and $0 < \alpha < 1$. It is easy to see that

- (i) $|x|_v = 0$ if and only if $x = 0$.
- (ii) $|xy|_v = |x|_v + |y|_v$.
- (iii) $|x + y|_v \leq \max\{|x|_v, |y|_v\}$. (strong triangle inequality)

The above function is called a non-archimedean absolute value since the absolute value function $|x|_v$ defined by the valuation v over \mathcal{F} satisfies the strong triangle inequality (condition (iii)). In fact, this is typical of all function fields.

Now, the valuation v turns \mathcal{F} into a topological field (through the absolute value function). In particular, it makes sense to discuss boundedness, cauchy-ness, convergence of sequences and ultimately the completion of \mathcal{F} . \mathcal{F} is said to be complete if every cauchy (fundamental) sequence in \mathcal{F} converges to an element in \mathcal{F} . We denote the completion of \mathcal{F} by $\hat{\mathcal{F}}$ (i.e. \mathcal{F} + all limits of cauchy sequences in \mathcal{F}). It carries an added advantage that, this completion is easier to work with compared to the original field. Examples of complete fields include,

1. The completion of \mathbf{Q} with respect to v_p denoted by \mathbf{Q}_p is the field of p -adic numbers. Its ring of integers is denoted by \mathbf{Z}_p is called the ring of p -adic integers. $\mathfrak{K} := \mathbf{Z}_p / p\mathbf{Z}_p$ is the residue field of \mathbf{Z}_p and is isomorphic to \mathbf{F}_p a finite field of p elements.
2. The completion of \mathbf{Q} with respect to the usual absolute value $|\cdot|$ is \mathbf{R} .

In the next paragraph, we shall explain how to complete the field k at the place ∞ .

Recall that $A = \mathbf{F}_r[T]$ and $k = \mathbf{F}_r(T)$; set v_∞ to be the discrete valuation corresponding to the place ∞ . We defined $v_\infty(f) := -\deg(f)$ for every $f \in A$. Suppose that $\deg(f) = n$, then we can write $f(T) = T^n g(\frac{1}{T})$, where g is a polynomial with a non-zero constant term. If we set $U = \frac{1}{T}$, the prime $U \in \mathbf{F}_r[U] = \mathbf{F}_r[\frac{1}{T}]$ defines a discrete rank 1 valuation of k . Clearly, we see that $v_U(f) = v_U(U^{-n}g(U)) = -n$, and therefore the two valuations v_∞ and $v_{(\frac{1}{T})}$ coincide on A . This implies that the v_∞ and $v_{(\frac{1}{T})}$ also agree on the field of fractions k . Hence, the completion of k with respect to the place at infinity is the ring of the formal Laurent series in U , that is to say, $k_\infty := \mathbf{F}_r((U)) = \mathbf{F}_r((\frac{1}{T}))$. The elements of k_∞ regular at infinity are the power series in $\frac{1}{T}$, i.e. $\mathbf{F}_r[[\frac{1}{T}]]$ otherwise, they are irregular. In particular, the units at infinity are the power series in $\frac{1}{T}$ with non-zero constant term. If $0 \neq g \in \mathbf{F}_r((\frac{1}{T}))$, then we can write $g(T) = (\frac{1}{T})^N h(T)$ where h is a unit in $\mathbf{F}_r[[\frac{1}{T}]]$. In this situation, $v_\infty(g) = N$.

Proposition 4.1.5. *The only primes in k are the finite primes (those attached to the monic irreducibles in A) and the prime at infinity (corresponds to $\frac{1}{T}$). The degree of any finite prime is equal to the degree of the monic irreducible it corresponds to, and the degree of the prime at infinity is -1 . Moreover, $v_\infty(f) = -\deg(f)$ for all $f \in A$.*

In the non-archimedean analysis, the notions of convergence or divergence of series are defined by partial sums exactly as in the real or complex analysis. Unlike the classical archimedean theory, where $\lim_{j \rightarrow \infty} a_j = 0$ does not necessarily imply convergence of $\sum_j a_j$, in non-archimedean analysis, we have the series $\sum a_j$ converges if and only if $\lim_{j \rightarrow \infty} a_j = 0$.

Definition 4.1.6. Let \mathcal{F} be a complete field and $f(X) = \sum_{j=0}^{\infty} a_j X^j \in \mathcal{F}[[X]]$, then the order of convergence of f is $\rho(f) = -\lim_{j \rightarrow \infty} \inf\{\frac{v(a_j)}{j}\}$.

Let $v \in \mathbf{R}$, \mathcal{F} be a complete and algebraically closed field, we define (i) a closed disc in \mathcal{F} as $B := \{x \in \mathcal{F} : v(x) \geq v\}$, (ii) an open disc as $B^0 := \{x \in \mathcal{F} : v(x) > v\}$ and (iii) a circle of radius v by $C := \{x \in \mathcal{F} : v(x) = v\}$. With these notions, we can easily discuss topological questions on this field. As an immediate application of this, we describe the Newton polygon. This tool enables us to find information about the size and distribution of roots of a polynomial $f(X)$ with coefficients lying in the discrete valued field \mathcal{F} .

Definition 4.1.7. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathcal{F}[[X]]$ and $S = \{(i, v(a_i)) \in \mathbf{N} \times \mathbf{Z}\} \subset \mathbf{R}^2$. Then, the lower convex hull of S is called the Newton polygon of $f(X)$ denoted by $\text{NP}(f)$.

Let m_j the slope of the j^{th} side of $\text{NP}(f)$. It is clear, the point $(i, v(a_i))$ lies on the line $y + v(X)x = v(a_i X^i)$. If $\{m_j\}$ is the sequence of slopes of $\text{NP}(f)$, then $\{m_j\}$ is monotonically increasing and converges to $-\rho(f)$. We shall need the theorem below.

Theorem 4.1.8. Let $v > \rho(f)$, if there exists no side of $\text{NP}(f)$ with slope $-v$, then there are no zeros of $f(X)$ on $v(X) = v$, otherwise $f(X)$ has exactly m zeros on $v(X) = v$ where m is the length of the projection of the $\text{NP}(f)$ side with slope $-v$ onto the X -axis.

Proof. ([19], Theorem 2.9). □

Example 4.1.9. Let $f(X) = \sum_{i=0}^n a_i X^i \in \mathbf{Q}_p[X]$ be Eisenstein, i.e. $v_p(a_n) = 0$, $v_p(a_i) > 0$ for $1 \leq i < n$ and $v_p(a_0) = 1$. One observes without any effort, that the Newton polygon of $f(X)$ is just the line segment via $(0, 1)$ and $(n, 0)$. It follows that $f(X)$ has n roots λ , and $v_p(\lambda) = \frac{1}{n}$. Since every Eisenstein polynomial is irreducible, it follows that adjoining any root of $f(X)$ to \mathbf{Q}_p results into a totally ramified extension of degree n .

Proposition 4.1.10. If $f(X)$ is entire with no zeros, then $f(X)$ is constant.

Proof. ([10], Proposition 2.13) Suppose $\rho(f(X)) = -\infty$, and $f(X)$ is non-constant, then $\text{NP}(f(X))$ has at least one finite non vertical side and that means it has a root. □

Theorem 4.1.11 (Weierstrass preparation theorem). Let $f(X)$ be a non-constant entire function and $\{\lambda_1, \dots, \lambda_t, \dots\}$ be its non-zero roots in \mathcal{F} . Then $-\infty = \lim_{t \rightarrow \infty} v(\lambda_t)$ and there is a non-zero constant $c \in \mathcal{F}$ such that

$$f(X) = cX^n \prod_{t=1}^{\infty} \left(1 - \frac{X}{\lambda_t}\right), \quad n = \text{ord}_{X=0} f(X).$$

Conversely, if $-\infty = \lim_{t \rightarrow \infty} v(\lambda_t)$, then the above product defines an entire function.

Proof. ([10], Theorem 2.14) (\Leftarrow) Such products define entire functions. (\Rightarrow) Now, suppose $f(X)$ is a non-constant entire function. We formulate $f^*(X) = X^n \prod_{t=1}^{\infty} (1 - \frac{X}{\lambda_t})$, where $n = \text{ord}_{X=0} f(X)$. Since $f(X), f^*(X)$ have the same zeros every where, $g(X) = \frac{f(X)}{f^*(X)}$ is entire with no zeros therefore a constant function by proposition 4.1.10. \square

4.2 The Carlitz exponential

Let us now fix our notation to be used from now onwards, $r = p^l, A = \mathbf{F}_r[T], k = \mathbf{F}_r(T)$, although this is not canonical since $k = \mathbf{F}_r(\frac{aT+b}{cT+d})$, with $ad - bc \neq 0, a, b, c, d \in \mathbf{F}_r$ can also work well. We provided the completion of k , by choosing a place ∞ of k and setting $v_{\infty} : k \rightarrow \mathbf{Z} \cup \{\infty\}$ to be the valuation associated with $\frac{1}{T}$ as its uniformiser ($v_{\infty}(\frac{1}{T}) = 1$). Unlike the archimedean place at infinity in \mathbf{Q} , this (' ∞ ' of k) induces a discrete valuation ring. We shall denote the associated completion k_{∞} of k by K . Therefore, K is complete and locally compact in the $\frac{1}{T}$ topology but not algebraically closed. Since the multiplicative representatives of the residue classes form subfield of \mathbf{F}_r , K is called a local field, its local ring at ∞ is isomorphic to $\mathbf{F}_r[[\frac{1}{T}]]$. Alternatively, we view k as a field of functions on quotient space \mathbf{P}^1 over \mathbf{F}_r while A is the sub-ring of all functions regular outside ∞ . (have ∞ as the only pole).

We are now aware of the following basic analogy: $A \sim \mathbf{Z}, k \sim \mathbf{Q}$ and $K \sim \mathbf{R}$. Indeed, both A and \mathbf{Z} possess division algorithms and A is discrete inside K as is \mathbf{Z} in $\mathbf{R} = \mathbf{Q}_{\infty}$.

Proposition 4.2.1. *A is a discrete subring of K . Moreover, K/A is compact.*

Proof. ([10], Proposition 3.1.1) Let $a \in A$ with $v_{\infty}(a) > 0$, this implies, we must have $a = 0$. Indeed, if $v_{\infty}(a) > 0$, then a has a zero at $\infty \in \mathbf{P}^1$; therefore, a is regular every where. By theorem 4.1.10, a is a constant function with zeros at ∞ , that is to say $a = 0$. The discreteness of A in K follows from the fact that v_{∞} is a discrete valuation. To see the co-compactness of A , we consider the polar part of a Laurent series in $\frac{1}{T}$, which is precisely a polynomial in T . Thus, K/A is isomorphic to $\frac{1}{T} \mathbf{F}_r[[\frac{1}{T}]]$. The ring $\mathbf{F}_r[[\frac{1}{T}]]$ is the inverse (projective) limit of the finite rings $\mathbf{F}_r[[\frac{1}{T}]] / \langle \frac{1}{T^n} \rangle$ as n tends to ∞ and is compact. Thus, so is $K/A \cong \frac{1}{T} \mathbf{F}_r[[\frac{1}{T}]]$. \square

If we let \bar{K} be the algebraic closure of K , we are tempted to think of \bar{K} as being analogous to \mathbf{C} in the sense that it is algebraically closed. However, $[\bar{K} : K] = \infty$, so it is neither complete nor locally compact. We resolve the completeness problem by taking the completion of \bar{K} with respect to v_{∞} to get \mathbf{C}_{∞} . This has an added advantage that, \mathbf{C}_{∞} is still algebraically closed (analogous to \mathbf{C} in this sense), however it is still not locally compact.

For any $n \in \mathbf{N}$, we define $A_n := \{f \in A : \deg(f) < n\}$, the \mathbf{F}_r^n -subspace of polynomials with degree strictly less than n . Most importantly, A_n is an \mathbf{F}_r -module of size r^n and $A = \bigcup_{n \geq 0} A_n$. We do our usual trick of translating an algebraic structure into a polynomial.

Definition 4.2.2. We set $e_0(z) = z$ and for $n > 0$,

$$e_n(z) := \prod_{f \in A_n} (z - f) = \prod_{f \in A_n} (z + f).$$

It is trivial that $e_n(z)$ is an \mathbf{F}_r -linear polynomial (from the theory of additive polynomials) and therefore $e_n \in A\{\tau\}$. We now attempt give the coefficients of $e_n(z)$ in a closed form. We begin by asking how might one compute a factorial in A ? In his memorable article [8] of 1932, Carlitz explicitly answered this question, motivating the following definitions.

Definition 4.2.3. Let $i > 0$. We set,

- (i) $[0] = 1$ and $[i] = T^{r^i} - T$.
- (ii) $D_0 = 1$ and $D_i = [i][i-1]^r \cdots [1]^{r^{i-1}}$.
- (iii) $L_0 = 1$ and $L_i = [i][i-1] \cdots [1]$.

Proposition 4.2.4. For $i \geq 1$, we have

- (i) $[i]$ is the product of all primes in A of degree dividing i .
- (ii) D_i is the product of all polynomials in A^+ of degree i .
- (iii) L_i is the least common multiple of polynomials of degree i .

Proof. ([10], Proposition 3.1.6) □

The numbers $[i], D_i, L_i$ are fundamental in the arithmetic of $\mathbf{F}_r[T]$ [10], (in fact D_i is the analogue of the classical factorial). Some of their properties include, (a) $\deg([i]) = r^i$, (b) $\deg(D_i) = ir^i$ and (c) $\deg(L_i) = r \cdot \frac{(r^i-1)}{(r-1)}$. Moreover, it is not hard to show that the product of all non-zero polynomials in A of degree $< i$ is $(-1)^i \frac{D_i}{L_i}$. Carlitz derived all the above results using what we now call ‘the analytic approach’, he used it to prove,

Theorem 4.2.5 (Carlitz).

$$e_n(z) = \sum_{i=0}^n (-1)^{n-i} \left(\frac{D_n}{D_i L_{n-i}^{r^i}} \right) z^{r^i}.$$

For an explicit derivation of this, one can read [10] or [19], they handle it fair enough.

Remark 4.2.6. The coefficients of $e_n(z)$ are integral i.e. $\frac{D_n}{D_i L_{n-i}^{r^i}} \in A$. Indeed, this is a consequence of the expansion for $e_n(z)$ in definition 4.2.2.

Remark 4.2.7. If we further divide both sides of theorem 4.2.5 by $(-1)^n \frac{D_n}{L_n}$, we obtain

$$E_n(z) := (-1)^n \frac{L_n}{D_n} e_n(z) = z \prod_{0 \neq f \in A_n} \left(1 - \frac{z}{f}\right) = \sum_{i=0}^n (-1)^i \frac{z^{r^i}}{D_i} \left(\frac{L_n}{L_{n-i}^{r^i}}\right).$$

To obtain the Carlitz exponential, one has to evaluate the limit of $E_n(z)$ as $n \rightarrow \infty$. The LHS converges to an entire function and so we try to compute the limit of the RHS. Following Carlitz, define \mathbf{i} to be some fixed $(r-1)^{\text{st}}$ root of $-[1]$ in \bar{K} . For $i \geq 0$, put

$$\pi_i = \frac{\mathbf{i}^{r^i-1}}{L_i} = \frac{\prod_{j=0}^{i-1} [1]^{r^j}}{\prod_{j=1}^i [j]} = \prod_{j=1}^{i-1} \left(\frac{[j+1] - [j]}{[j+1]}\right) = \prod_{j=1}^{i-1} \left(1 - \frac{[j]}{[j+1]}\right).$$

Then, $\pi = \lim_{i \rightarrow \infty} \pi_i$ exists in K and has the infinite product representation

$$\pi = \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right).$$

We may now re-write $E_n(z)$ (carefully) as

$$E_n(z) = \sum_{i=0}^n (-1)^i \frac{z^{r^i}}{D_i} \left(\frac{L_n}{L_{n-i}^{r^i}}\right) = \frac{1}{\mathbf{i} \pi_n} \sum_{i=0}^n (-1)^i \frac{z^{r^i}}{D_i} (\mathbf{i} \pi_{n-i})^{r^i}.$$

Now $\lim_{n \rightarrow \infty} \pi_{n-i} = \pi$ encourages us to believe that

$$E_{\infty}(z) = \frac{1}{\bar{\pi}} \sum_{i=0}^{\infty} (-1)^i \frac{\bar{\pi}^{r^i}}{D_i} z^{r^i}, \text{ where } \bar{\pi} := \mathbf{i} \pi = (-1)^{\frac{1}{r-1}} \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right).$$

$\bar{\pi}$ is analogous to “ $2\pi i$ ”, the period of the classical exponential function. Moreover, one easily sees that $\bar{\pi}$ is well defined up-to multiplication by $\alpha \in A^*$. L. Wade (1942) showed that the Carlitz period $\bar{\pi}$ is transcendental over k . If we now replace, z with $\frac{z}{\bar{\pi}}$, we obtain

$$e_C(z) := z \prod_{0 \neq f \in \bar{\pi}A} \left(1 - \frac{z}{f}\right) = \sum_{i=0}^{\infty} (-1)^i \frac{z^{r^i}}{D_i}.$$

See [19], Chapter 3 for details. Carlitz showed that $e_{\bar{\pi}A}(z)$ satisfied “complex multiplications” under the action of elements of A . For example, that $e_C(Tz) = Te_C(z) - e_C(z)^r$. In [11], Hayes replaced the ‘minus’ sign with a ‘plus’ sign and showed that the two multiplications yield isomorphic modules over \mathbf{C}_{∞} (see section 4.3). Its associated exponential is,

Definition 4.2.8 (The Carlitz exponential).

$$e_C(z) := \sum_{j=0}^{\infty} \frac{z^{r^j}}{D_j}, \text{ for any } z \in \mathbf{C}_{\infty}.$$

Its properties are very similar to those of the complex exponential. We demonstrate this in a detailed fashion because it is the starting point of the many analogues to be discussed.

Proposition 4.2.9. *As a function on \mathbf{C}_{∞} , $e_C(z)$ is \mathbf{F}_r -linear, surjective and entire.*

Proof. We proceed in 3 parts,

1. (Linearity). For $z_1, z_2 \in \mathbf{C}_{\infty}$, we have

$$e_C(\alpha z_1 + \beta z_2) = \sum_{j=0}^{\infty} \frac{(\alpha z_1 + \beta z_2)^{r^j}}{D_j} = \alpha \sum_{j=0}^{\infty} \frac{z_1^{r^j}}{D_j} + \beta \sum_{j=0}^{\infty} \frac{z_2^{r^j}}{D_j} = \alpha e_C(z_1) + \beta e_C(z_2).$$

2. (Entire). We must show that the order of convergence of the series is ∞ . Now

$$\rho(e_C(z)) = - \liminf_{j \rightarrow \infty} \left\{ \frac{v(\frac{1}{D_j})}{r^j} \right\} = \liminf_{j \rightarrow \infty} \left\{ \frac{v(D_j)}{r^j} \right\} = \liminf_{j \rightarrow \infty} \left\{ \frac{j r^j}{r^j} \right\} = \infty.$$

3. (Surjection). For any $\alpha \in \mathbf{C}_{\infty}$, the function $g(z) = -\alpha + e_C(z)$ has a zero in \mathbf{C}_{∞} since $e_C(z)$ is non-constant entire function on \mathbf{C}_{∞} . Therefore, $e_C(z)$ is a surjection. □

Since $e_C(z)$ is separable and \mathbf{F}_r -linear, corollary 3.2.2 implies that, Λ_C is an \mathbf{F}_r -module.

Definition 4.2.10. *A subset $\Gamma \subseteq \mathbf{C}_{\infty}$ is strongly discrete if it has a finite intersection with every open ball $B_{\varepsilon}(0)$. Γ has rank s if $\Gamma K \cong K^s$ i.e. K -linear span of Γ has dimension s as a K -vector space. A lattice Γ of rank s in \mathbf{C}_{∞} is a strongly discrete A sub-module of rank s , (since $A \subset \mathbf{C}_{\infty}$, $(\mathbf{C}_{\infty}, +)$ is an A module in the most natural way).*

To each strongly discrete subset $\Gamma \subseteq \mathbf{C}_{\infty}$, we associate an exponential function,

$$e_{\Gamma}(z) = \begin{cases} \prod_{h \in \Gamma} \left(1 - \frac{z}{h}\right), & \text{if } 0 \notin \Gamma, \\ z \prod_{h \in \Gamma} \left(1 - \frac{z}{h}\right), & \text{if } 0 \in \Gamma. \end{cases}$$

Note, if Γ is finite, then $e_{\Gamma}(z) \in \mathbf{C}_{\infty}[z]$ is just a polynomial.

Proposition 4.2.11. $\Lambda_C = \{\lambda \in \mathbf{C}_{\infty} : e_C(\lambda) = 0\}$ is a discrete rank one free A -module,

$$e_{\Lambda_C}(z) = z \prod_{\lambda \in \Lambda_C \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) = e_C(z).$$

Proof. By our construction of $e_C(z)$, we have $\Lambda_C = \text{Ker}(e_C(z)) = \text{Ker}(e_{\bar{\pi}A}(z)) = \bar{\pi}A$, a free A -module of rank one. The discreteness of Λ_C follows from the discreteness of A . Now Λ_C is a strongly discrete rank one A -lattice and the exponential function associated to it is

$$e_{\Lambda_C}(z) = z \prod_{\lambda \in \Lambda_C \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right).$$

By the Weierstrass preparation theorem, tells us that $e_{\Lambda_C}(z)$ is entire, with Λ_C as its set of zeros, and therefore $e_{\Lambda_C}(z)$ is separable. Λ_C is an A -module, (therefore an \mathbf{F}_r -vector space) and $e_{\Lambda_C}(z)$ separable, so $e_{\Lambda_C}(z)$ must be \mathbf{F}_r -linear and surjective as a map from $\mathbf{C}_\infty \rightarrow \mathbf{C}_\infty$. This implies that, $e_{\Lambda_C}(z)$ has a series expansion of the form $e_{\Lambda_C}(z) = \sum_{i=0}^{\infty} a_i z^i$. From the product expansion of $e_{\Lambda_C}(z)$, we get $a_0 = 1$. Now the functions $e_C(z)$ and $e_{\Lambda_C}(z)$ have the same roots; since $D_0 = 1$, we have $e'_C(z) = 1 = e'_{\Lambda_C}(z)$ yielding the second equality. \square

Corollary 4.2.12. $e_C(z)$ is Λ_C -periodic.

Proof. By \mathbf{F}_r -linearity of $e_C(z)$, so $e_C(z + \lambda) = e_C(z) + e_C(\lambda) = e_C(z)$ for all $\lambda \in \Lambda_C$. \square

We have already seen that $\bar{\pi} \in \mathbf{C}_\infty$ such that $\bar{\pi}A$ is the set of roots of the Carlitz exponential. This is analogous to $2\pi i\mathbf{Z}$, the kernel of the usual complex exponential. A keen reader can now reflect on the obvious analogies between the product expansion of $e_C(z)$ and the familiar Weierstrass product expansion of $e^{2\pi iz} - 1$ as a function on \mathbf{C} .

4.3 The Carlitz module

We use $e_C(z)$ to describe a new module action of A on \mathbf{C}_∞ .

Lemma 4.3.1. Let $z \in \mathbf{C}_\infty$, then $e_C(Tz) = Te_C(z) + e_C(z)^r$.

Proof. $e_C(Tz) - Te_C(z) = \sum_{i=0}^{\infty} (T^{r^i} - T) \frac{z^{r^i}}{D_i} = \sum_{i=1}^{\infty} \frac{z^{r^i}}{D_{i-1}} = \left(\sum_{i=0}^{\infty} \frac{z^{r^i}}{D_i}\right)^r = e_C(z)^r$. \square

Proposition 4.3.2. Let $a \in A$ with $a = \sum_{j=0}^n \alpha_j T^j$ and $\alpha_n \neq 0$, there exists $a_1, \dots, a_n \in A$ such that for all $z \in \mathbf{C}_\infty$, we have

$$e_C(az) = \sum_{j=0}^n a_j e_C(z)^{r^j} = \phi_a(e_C(z)),$$

$a_n = \alpha_n$, $\deg(a_j) = r^j(n - j)$ and $\phi_a(e_C(z))$ an additive polynomial in $e_C(z)$.

Proof. By \mathbf{F}_r -linearity, it suffices to investigate the special case where $a = T^d$ is monic of degree d . This is done by induction on d . For $d = 1$, we have $\phi_T(X) = TX + X^r$, therefore $a_0 = T$ of degree $r^0(1 - 0) = 1$ and $a_1 = 1$ of degree $r^1(1 - 1) = 0$. Hence, the result is true for $d = 1$. In order to proceed, we need to obtain the recursive formula for a_j first.

Assume, (induction hypothesis) the result is true for all monomials T^s of degree $s \leq d-1$, then $\phi_{T^d}(X) = \phi_T(\phi_{T^{d-1}}(X)) = T\phi_{T^{d-1}}(X) + (\phi_{T^{d-1}}(X))^r$ and so $\phi_{T^d}(X) = \sum_{j=0}^d \phi_{T^d}^{(j)} X^{r^j}$ exists. Isolating the coefficients of X^{r^j} on both sides, we obtain the following recursive formula; $\phi_{T^d}^{(j)} = T\phi_{T^{d-1}}^{(j)} + (\phi_{T^{d-1}}^{(j-1)})^r$ for $j > 0$. Using the induction step at d , the degree of the first term on the RHS is $1 + r^j(d-j-1)$ and that of the second term on the RHS is $r^j(d-j)$. Since $j > 0$, the second term has larger degree compared to the first. Therefore, $a_j := \phi_{T^d}^{(j)}$ has degree $r^j(d-j)$. Also note, for $a = T^j$, $\deg(a_j) = 0$ (in particular, the leading coefficient of T^j) and for $j > 0$, we have $\deg(a_j) > 0$. Since $a_j \in A$, we have $a_j = 0$ for all $j > n$.

We complete this proof using \mathbf{F}_r -linearity of ϕ . For $a = \sum_{j=0}^n \alpha_j T^j \in A$ with $\alpha_j \in \mathbf{F}_r$ and $\alpha_n \neq 0$. By \mathbf{F}_r -linearity, it follows trivially that $\phi_a(X) = \sum_{i=0}^n \alpha_i \phi_{T^i}^{(j)} X^{r^i}$, from which one notices; $\deg(a_j) = \deg(\phi_a^{(j)}) = r^j(n-j)$ since it is the non-zero term of highest degree. Further-still, by linearity one notices that $a_0 = a, a_n = \alpha_n$ and $a_j = 0$ for $j > n$. This also shows that, the a_j 's can be computed recursively, (we shall demonstrate this later on). \square

The polynomial ϕ_a is called the Carlitz polynomial corresponding to the $a \in A$. It may be given in two forms, as a polynomial in $A[X]$ or $A\{\tau\}$. For-example, one can easily show that $e_C(Tz) = Te_C(z) + e_C(z)^r = \phi_T(e_C(z))$, so $\phi_T(X) = TX + X^r$ or simply $\phi_T = T\tau^0 + \tau \in \mathbf{C}\{\tau\}$.

Definition 4.3.3. Let $\{a_j\}$ be as above and $\deg(a) = n$, then we set $\phi_a = a\tau^0 + \sum_{j=1}^n a_j \tau^j$.

ϕ_a is called the a^{th} Carlitz polynomial in $\mathbf{C}_\infty\{\tau\}$. Actually, the coefficients of $\phi_a(X)$ considered as functions of rank one A -lattices turn out to be modular functions. We also see that, the a^{th} Carlitz polynomial can be given as a polynomial in $k\{\tau\}$ or $k[X]$.

Proposition 4.3.4. $\phi : A \rightarrow A\{\tau\}$, $a \mapsto \phi_a$, is a monomorphism of \mathbf{F}_r -algebras.

Proof. The map $a \mapsto \phi_a$ is \mathbf{F}_r -linear and injective since $\text{Ker}(\phi) = \{0\}$. We show, ϕ is a map between \mathbf{F}_r -algebras i.e. $\phi_{a+b} = \phi_a + \phi_b$ and $\phi_{ab} = \phi_a \cdot \phi_b$ where \cdot is multiplication in $k\{\tau\}$ + is trivial and $\phi_{ab}(e_C(z)) = e_C(a(bz)) = \phi_a(e_C(bz)) = \phi_a(\phi_b(e_C(z))) = (\phi_a \cdot \phi_b)(e_C(z))$. \square

The map ϕ defined by $\phi(a) = \phi_a$, is the **Carlitz module**. Algebraically, since $e_C(z)$ turns \mathbf{C}_∞ into \mathbf{C}_∞ (as additive groups) and lattice $\Lambda_C \subset \mathbf{C}_\infty$ is an abelian group carrying the usual A -module structure, we get the famous commutative diagram with exact rows.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \Lambda_C & \longrightarrow & \mathbf{C}_\infty & \xrightarrow{e_C(z)} & \mathbf{C}_\infty \longrightarrow 0 \\
 & & \downarrow a & & \downarrow a & & \downarrow \phi_a \\
 0 & \longrightarrow & \Lambda_C & \longrightarrow & \mathbf{C}_\infty & \xrightarrow{e_C(z)} & \mathbf{C}_\infty \longrightarrow 0
 \end{array}$$

For commutation in the right square, we require that the fundamental functional equation,

$$e_C(az) = \phi_a(e_C(z)),$$

that is to say,

$$e_C(az) = ae_C(z) + \sum_{j=1}^n a_j e_C(z)^{r^j} = \phi_a(e_C(z)).$$

Replacing $e_C(z)$ by X , we get $\phi_a(X) = aX + \sum_{j=1}^n a_j X^{r^j} = (a\tau^0 + \sum_{j=1}^n a_j \tau^j)(X)$. In this way, we can view ϕ as the ring homomorphism from a nice commutative ring A to a non-commutative ring $A\{\tau\}$, or as an action that gives \mathbf{C}_∞ a new A -module structure.

We now give a very brief introduction to the generalisation of the Carlitz modules. This is for purposes of understanding the Carlitz module as a rank one Drinfeld module.

Definition 4.3.5. *A Drinfeld A -module over k consists of an \mathbf{F}_r -algebra homomorphism $\rho : A \rightarrow k\{\tau\}$ such that for all $a \in A$, the constant term of ρ_a is a . Moreover, we require that the image of ρ is not contained in k i.e. there is atleast one $a \in A$ such that $\rho_a \notin A$.*

A Drinfeld module ρ is said to be of rank s if $\rho_T = T\tau^0 + c_1\tau + \dots + c_s\tau^s$ with $c_s \neq 0$. It is now obvious to see why one says a Carlitz module is a rank one Drinfeld A -module. Let ϕ and ϕ' be two Drinfeld A -modules over k . An isogeny from ϕ to ϕ' is a twisted polynomial $g \in k\{\tau\}$ such that $g\phi_a = \phi'_a g$ for all $a \in A$. If $h_1 : \phi_1 \rightarrow \phi_2$ and $h_2 : \phi_2 \rightarrow \phi_3$ are isogenies, then clearly the product of isogenies $h = h_2 \circ h_1 : \phi_1 \rightarrow \phi_3$ is also an isogeny. Drinfeld A -modules over k constitute a category $\text{Drin}_A(k)$ in which the morphisms are the isogenies. So an isomorphism between modules will be any invertible isogeny. Since the only invertible polynomials in $k\{\tau\}$ are constants, $\phi \cong \phi'$ if and only if there is a $g \in k^*$ such that $g\phi_a = \phi'_a g$ for all $a \in A$. In particular, the two modules $\phi_T = T\tau^0 - \tau$ and $\phi'_T = T\tau^0 + \tau$ are isomorphic as elements of $\text{Drin}_A(\mathbf{C}_\infty)$ since there is an element $\xi \in \mathbf{C}_\infty$, where ξ is the $(r-1)^{\text{st}}$ root of -1 , that acts as an isogeny. i.e. $\xi\phi_T = \xi T\tau^0 - \xi\tau = T\tau^0\xi + \tau(-\xi)^{\frac{1}{r}} = T\tau^0\xi + \tau\xi = \phi'_T\xi$. It is important to note that, had we defined the Carlitz modules as just elements of $\text{Drin}_A(k)$, then for r odd, they would not be isomorphic because $\xi \notin k$.

Although for the Carlitz module, we constructed the exponential function first, and then its lattice, in the general theory of Drinfeld modules, it is normally done the other way round. Given a lattice Γ (of arbitrary rank), we can construct the associated exponential function $e_\Gamma(z)$ and the corresponding Drinfeld module ρ for example, in the case of the Carlitz module, Λ_C is the lattice, $e_C(z)$ the associated exponential and $\rho := \phi$, the Drinfeld module. A lot can be said about Drinfeld modules, but this is not the subject for the thesis. We now give a recursive formula for the coefficients, $\{a_j\}$ of the a^{th} Carlitz polynomial.

Lemma 4.3.6. *Let $a \in A$ be monic of degree n and $\phi_a = \sum_{j=0}^n a_j \tau^j$, then*

$$a_0 = a, a_1 = \frac{a_0^r - a_0}{T^r - T}, a_2 = \frac{a_1^r - a_1}{T^{r^2} - T}, \dots, a_i = \frac{a_{i-1}^r - a_{i-1}}{T^{r^i} - T}, \dots, a_n = 1.$$

Moreover, if $a = \alpha f$ for $\alpha \in \mathbf{F}_r^*$ and f monic of degree n , then $a_n = \alpha$.

Proof. ([10], Proposition 3.3.10) Write $\phi_a = a\tau^0 + \chi_a$, where $\chi_a \in A\{\tau\}$ (remaining part of ϕ_a). So $\chi_T = \tau$ together with $\phi_a \phi_T = \phi_T \phi_a \in k\{\tau\}$, where $\phi_T = T\tau^0 + \tau$. In principle,

$$\begin{aligned} (a\tau^0 + \chi_a)(T\tau^0 + \tau) &= (T\tau^0 + \tau)(a\tau^0 + \chi_a) \\ Ta\tau^0 + a\tau + \sum_{j=1}^n T^{r^j} a_j \tau^j + \sum_{j=1}^n a_j \tau^{j+1} &= Ta\tau^0 + a^r \tau + \sum_{j=1}^n Ta_j \tau^j + \sum_{j=1}^n a_j^r \tau^{j+1} \\ \sum_{j=0}^n (T^{r^j} - T) a_j \tau^j &= \sum_{j=1}^{n+1} (a_{j-1}^r - a_{j-1}) \tau^j. \end{aligned}$$

The result follows upon equating the coefficients of τ^j on both sides of the above equation. With the constraints $a_0 = a$ and $a_n = 1$ if a is monic; otherwise $a_n = \text{LC}(a) = \alpha \in \mathbf{F}_r^*$. \square

This is the lemma behind algorithm 1. Algorithm 2 uses the fact that ϕ is a homomorphism. see Appendix A. With this lemma, we are in position to calculate any $\phi_a(X)$ (in principle, this formula works but the level of difficulty and complexity increases with $\deg(a)$).

Remark 4.3.7. *Let P be a prime polynomial, then*

- (a) $\phi_P = \tau^n + a_{n-1} \tau^{n-1} + \dots + a_1 \tau + a_0 \tau^0$ with $P \mid a_i$ for $1 \leq i \leq n-1$ and $P^2 \nmid a_0$.
To see this easily compute the a_i 's modulo P , also see that $P^2 \nmid a_0 = P \equiv 0 \pmod{P}$.
- (b) $a_i \neq 0$ for $i = 1, \dots, n$, $a_n = \alpha$ and $a_{n+1} = a_{n+2} = \dots = 0$. ([10], Proposition 3.3.10)

It is now a good time to describe a procedure for obtaining coefficients of $\phi_{T^s}(X)$ in $\mathbf{F}_r[T]$. This is based on the fact that, Carlitz polynomials are indeed additive.

Proposition 4.3.8. *Let $\phi_{T^n}(X) = \sum_{s=0}^{r^n} a_{T^n}(s) X^s$, then*

$$a_{T^n}(s) = \begin{cases} 0, & s \neq r^t, \\ 1, & s = r^n, \\ a_{T^{n-1}}(r^{t-1})^r + T \cdot a_{T^{n-1}}(r^t), & s = r^t. \end{cases}$$

Proof. Define $\phi_{T^n}(X) = \sum_{s=0}^{r^n} a_{T^n}(s) X^s$ or simply $\phi_{T^n}(X) = \sum_{s=0}^{r^n} a_s X^{r^s}$. The first cases are trivial, so we investigate the last case where $s = r^t$. This case is proved by doing an induction on the degree of T^n , and considering all the previous situations. \square

Using proposition 4.3.8, we actually show that, obtaining of coefficients of $\phi_{T^n}(X)$ is similar to that of obtaining coefficients of a binomial expansion using the Pascal's triangle. The only difference is that; the addition of previous elements is governed by Carlitz action.

We illustrate this below via what we have called the "Carlitz's triangle".(similar to Pascal's triangle). In fact, when evaluated at $T = 1$, one obtains Pascal's 1 triangle.

$$\begin{array}{ccccccc}
 m = 1: & & & & & & 1 \\
 m = T: & & & & 1 & & T \\
 m = T^2: & & 1 & & T^r + T & & T^2 \\
 m = T^3: & 1 & T^{r^2} + T^r + T & & T^{2r} + T^{r+1} + T^2 & & T^3
 \end{array}$$

If $[n, j]$ represents the coefficient of X^{r^j} in $\phi_{T^n}(X)$, (the element in the n^{th} row and j^{th} column of the Carlitz triangle), then we have the relation $[n, j] = [n - 1, j]^r + [n - 1, j - 1]T$. Here we count the columns from the right. I have not yet found any interesting mathematics embedded in this triangle. This might be due to the absence of symmetry in the coefficients. For-example one can no-longer obtain the Sierpinski triangles, the normal combinatorics and therefore probability interpretations are totally lost. But like earlier on noted, all the Pascal's triangle properties are recovered when one evaluates the triangle at $T = 1$. This triangular construction can be done for powers of a , for any $a \in A$ (the only disadvantage is complexity of computations grows rapidly). A similar triangle is obtained when one uses $\phi_T = T\tau^0 - \tau$. The only difference is a factor of -1 on the coefficients in odd positions.

Consider the A -module, \mathbf{C}_∞ , we define the torsion sub-module of \mathbf{C}_∞ as

$$\Lambda := \{\lambda \in \mathbf{C}_\infty : \phi_a(\lambda) = 0 \text{ for some } 0 \neq a \in A\}.$$

For each non zero $a \in A$, we define $\Lambda[a] := \Lambda_a = \{\lambda \in \mathbf{C}_\infty : \phi_a(\lambda) = 0\}$, the set of a -torsion points. Proposition 4.3.10 shows that Λ_a is actually isomorphic to A/aA as a module and so any generator of Λ_a as an A -module is called an a^{th} primitive division point (root of $\phi_a(X)$). If $\alpha \in \mathbf{F}_r^*$, then $\Lambda_a = \Lambda_{\alpha a}$, since $\phi_{\alpha a} = \phi_\alpha \phi_a = \alpha \phi_a$. In later chapters, we shall assume a to be monic, hence Λ_a entirely depends only on the principal ideal $\langle a \rangle$. If we adjoin Λ_a to k , we obtain what is called the Carlitz cyclotomic function field denoted by $K_{C,a} := K_a = k(\Lambda_a)$. There is another way of obtaining cyclotomic extensions and this is by adjoining more roots of unity. However, this yields constant field extensions. Since $\phi_a(X)$ and $\phi'_a(X) = a$ are co-prime, $\phi_a(X)$ is separable a polynomial with Λ_a as its set of roots. It follows that, K_a/k is a Galois extension with Galois group $\text{Gal}(K_a/k)$.

If λ is a primitive a torsion point, then for each $\sigma \in \text{Gal}(K_a/k)$, we have $\phi_a(\sigma\lambda) = 0$.

Lemma 4.3.9. *Let $0 \neq a \in A$, $\Lambda \subseteq \mathbf{C}_\infty$ be an A -module. Suppose for each $b \mid a$, the sub-module Λ_b has $r^{s \deg(b)}$ elements. We have $\Lambda_a \cong (A/aA) \oplus \cdots \oplus (A/aA)$. (s times)*

Proof. ([18], Lemma 12.3) Consider the prime decomposition of a , $a = \alpha P_1^{e_1} \cdots P_t^{e_t}$, where $\alpha \in \mathbf{F}_r^*$ and the P_i 's run via the prime factors of a . By the structure theory of modules over PID's, we have the isomorphism $\Lambda_a \cong \Lambda_{P_1^{e_1}} \oplus \cdots \oplus \Lambda_{P_t^{e_t}}$. Let us consider the case $a = P^e$.

Suppose $a = P^e$ is a prime power with $e \geq 1$. Since Λ_{P^e} is a vector space over (A/PA) with $r^{s \deg(P)}$ elements, by our hypothesis, it follows that the dimension of Λ_P over A/PA is s (since $\#(A/PA) = r^{\deg(P)}$). It also follows from the structure of modules over PID's that

$$\Lambda_{P^e} \cong \Lambda_{P^{f_1}} \oplus \cdots \oplus \Lambda_{P^{f_s}} = (A/P^{f_1}A) \oplus \cdots \oplus (A/P^{f_s}A).$$

One must have $f_i \leq e$ for $1 \leq i \leq s$. We then have

$$\#\Lambda_{P^e} = r^{es \deg(P)} = r^{(\sum_{i=1}^s f_i) \deg(P)} = \#((A/P^{f_1}A) \oplus \cdots \oplus (A/P^{f_s}A)).$$

This can only occur if $f_i = e$ for all $i = 1, \dots, s$, therefore $\Lambda_{P^e} \cong (A/P^eA) \oplus \cdots \oplus (A/P^eA)$. By the chinese remainder theorem, we have $\Lambda_a \cong (A/aA) \oplus \cdots \oplus (A/aA)$. (s times). \square

Proposition 4.3.10. *Let $0 \neq a \in A$ and ϕ be the Carlitz module, then $\Lambda_a \cong A/aA$.*

Proof. For each $0 \neq a \in A$, $\#(\Lambda_a) = r^{\deg(a)}$ and $\phi_a(X) = aX + b_1X^r + \cdots + b_{\deg(a)}X^{r^{\deg(a)}}$ where $b_i \in A$ and $b_{\deg(a)} \neq 0$. Since $\phi_a(X)$ is separable, it follows that $\phi_a(X)$ has $r^{\deg(a)}$ distinct roots, which are the precise elements of Λ_a . \square

Chapter 5

Cyclotomic polynomials over k

In this chapter, we will define the analogue $\Phi_n(X)$ which is the Carlitz cyclotomic polynomial $\Phi_m(X)$, state its elementary properties over k and some of its applications. We will also state and prove results concerning their coefficients and heights. We shall end with a brief introduction to cyclotomic function fields with more emphasis paid to ramification.

5.1 Carlitz cyclotomic polynomials

Let $m \in A^+$ and $\phi_m(X)$ denote the m^{th} Carlitz polynomial (image of m under the Carlitz module ϕ) in the variable X . $\phi_m(X)$ plays a very important role in the study of algebraic function fields as does $g_n(X) = X^n - 1$ in the study of algebraic number fields. We defined Λ_m to be the set of all the m -torsion points of the Carlitz module ϕ , that is to say the set of roots of $\phi_m(X)$. Now since $\phi_m(X)$ is separable over \mathbf{C}_∞ , all the roots of $\Phi_m(X)$ are distinct.

In addition, $\phi_m(X)$ is additive, therefore Λ_m is an abelian group endowed with an A -module structure via the Carlitz action. Moreover, the set Λ_m carries a cyclic A sub-module structure with its generators as the primitive m -torsion points. In chapter 4, we showed Λ_m to be isomorphic to A/mA (as A -modules), that is to say, if λ is a Λ_m -generator, then the map $\kappa : A/mA \rightarrow \Lambda_m$ defined by $a + mA \mapsto a \cdot \lambda := \phi_a(\lambda)$ is the module isomorphism required.

Remark 5.1.1. *In the map $\kappa : A/mA \rightarrow \Lambda_m$, we have standard multiplication by elements of A/mA on the left and the Carlitz action on the right. Here, we have Λ_m , the additive A -module as the natural analogue to μ_n , which is a multiplicative \mathbf{Z} -module.*

If λ_m is a generator of Λ_m and $a \in A$ is co-prime to m , then $\phi_a(\lambda_m)$ is also a generator of Λ_m that is, the primitive m -torsion points are obtained by applying a co-prime Carlitz action on any Λ_m generator. This parallels the classical case, in which the generators of μ_n are obtained

by raising any primitive root to an integer l relatively prime to n . We denote the set of all Λ_m generators by Λ_m^* and later on we show that, in fact $\text{Aut}_k(\Lambda_m) \cong (A/mA)^*$.

Classically, the n^{th} cyclotomic polynomial $\Phi_n(X)$, is a certain factor of $X^n - 1$. Doing the same thing with the rational function field k and assuming that, the Carlitz cyclotomic polynomial is a factor of the Carlitz polynomial $\phi_m(X)$. It turns out that, almost all the properties of classical cyclotomic polynomials in chapter 1 have analogues over the k . With this brief background, we define the m^{th} Carlitz cyclotomic polynomial as follows.

Definition 5.1.2. *Let $m \in A^+$, the m^{th} Carlitz cyclotomic polynomial over k is the monic polynomial whose roots are precisely all the primitive m^{th} torsion points in \mathbf{C}_∞ i.e.*

$$\Phi_m(X) = \prod_{\lambda \in \Lambda_m: \text{primitive}} (X - \lambda), \quad (5.1)$$

The m^{th} Carlitz inverse cyclotomic polynomial $\psi_m(X)$ is one whose roots are the non primitive m^{th} torsion points. So corollary 5.1.3 follows from the separability of $\phi_m(X)$.

Corollary 5.1.3. *Let $m \in A^+$, then $\psi_m(X)\Phi_m(X) = \phi_m(X)$.*

In this case, a primitive m -torsion point refers to any $\lambda_m \in \mathbf{C}_\infty$ that generates Λ_m as an A -module. We sometimes maintain the notation ' m^{th} ', just for identification although it does not make any sense classically. We also emphasize the name m^{th} Carlitz cyclotomic polynomial so as to distinguish it from the classical n^{th} cyclotomic polynomial. However, from now onwards, unless explicitly declared, we shall refer to $\Phi_m(X)$ as the m^{th} Carlitz cyclotomic polynomial. Later, we show that, $\Phi_m(X)$ has integral coefficients i.e. polynomials in the variable T and not just integers in \mathbf{Q} . Note that; whereas the roots of unity are in general complex numbers, here the "roots of unity" are 'complex' functions in \mathbf{C}_∞ . Here are some examples of a Carlitz polynomial and their corresponding Carlitz cyclotomic polynomial.

Example 5.1.4. *Let $\alpha, \beta \in \mathbf{F}_r$, then trivially $\phi_{\alpha T^0}(X) = \alpha X$ and $\Phi_{\alpha T^0}(X) = X$,*

$$\phi_{\alpha T + \beta}(X) = \alpha X^r + (\alpha T + \beta)X \text{ and } \Phi_{\alpha T + \beta}(X) = X^{r-1} + (T + \alpha^{-1}\beta).$$

Consider $A = \mathbf{F}_2[T]$ and $m = T^2 + T \in A$, then one can easily show $\phi_m(X) = X^4 + (T^2 + T + 1)X^2 + (T^2 + T)X$. Its set of roots is $\Lambda_m = \{0, T, T + 1, 1\}$, the m -torsion points. It is clear, $\Phi_m(X) = X + 1$, because $+1$ is the only generator of Λ_m as an A -module. One notices that, over $\mathbf{F}_2[T]$, $\Phi_1(X), \Phi_T(X), \Phi_{T+1}(X)$ and $\Phi_{T(T+1)}(X)$ are like $\Phi_1(X), \Phi_2(X)$ in the classical case; in the sense that, all have their roots in their corresponding integer rings i.e. $\mathbf{F}_2[T]$ and \mathbf{Z} . Like the classical cyclotomic polynomials, $\Phi_m(X)$ satisfies nice relations analogous to those encountered in chapter 1. We now explore some of these properties.

5.2 Properties of Carlitz cyclotomic polynomials

Proposition 5.2.1. *Let $m \in A^+$, then*

$$\begin{aligned}\phi_m(X) &= \prod_{d|m} \Phi_d(X), \text{ and} \\ \Phi_m(X) &= \prod_{d|m} (\phi_{\frac{m}{d}}(X))^{\mu(d)}.\end{aligned}$$

where μ is the polynomial version of the Möbius μ -function.

Proof. Since $\phi_m(X)$ is separable, the roots of $\phi_m(X)$ are exactly the Carlitz m -torsion points in \mathbf{C}_∞ . On the other hand, if λ_d is an m -torsion point of order d , (monic polynomial of least degree such that $\phi_d(\lambda_d) = 0$) then λ_d is a primitive d -torsion point, therefore λ_d is a root of $\Phi_d(X)$. But d divides m , hence λ_d is also a root to the RHS. Therefore, the polynomials on LHS and RHS have the same roots. Equality of both polynomials on the LHS and RHS follows from the fact that all the polynomials on both sides are monic and separable over \mathbf{C}_∞ . The next formula follows from the polynomial version of the Möbius inversion formula. \square

Proposition 5.2.2. *If $\phi_m(X)$ has a repeated root modulo a prime P , then P divides m . If P is a common prime factor of $\Phi_g(a)$ and $\Phi_m(a)$, where $a, g \in A$ with $\deg(g) < \deg(m)$ and g divides m , then $\phi_m(X)$ has a repeated root modulo P and P divides m .*

Proof. Assume there exists an $a \in A/PA$ such that $\phi_m(X) \equiv (X - a)^2 g(X) \pmod{P}$. Taking derivatives on both sides yields $m \equiv (X - a)(2g(X) + (X - a)g'(X)) \pmod{P}$. In particular, substituting a for X yields $m \equiv 0 \pmod{P}$ or equivalently P divides m .

For the second part, suppose P divides both $\Phi_{b_0}(a)$ and $\Phi_m(a)$ such that $b_0, a \in A$ together with $\deg(b_0) < \deg(m)$ and b_0 divides m . Trivially, $\phi_m(X)$ has a repeated root modulo P . So $0 \equiv \phi_m(a) \equiv \Phi_m(a)\Phi_{b_0}(a) \cdot (\text{other factors}) \pmod{P^2}$. Taking derivatives on both sides of the relation $\phi_m(X) = \prod_{d|m} \Phi_d(X)$ yields the following relation modulo P ,

$$m \equiv \Phi'_m(X)(\Phi_{b_0}(X) \cdot (\text{other factors})) + \Phi_m(X)(\Phi'_{b_0}(X) \cdot (\text{other factors}))' \pmod{P}.$$

Substituting a for X yields $m \equiv 0 \pmod{P}$ and so P divides m . \square

Definition 5.2.3. *Let m be a non zero polynomial in A , then the Carlitz order of $a \in A/mA$ is the monic polynomial d of least degree such that $\phi_d(a) \equiv 0 \pmod{m}$.*

Lemma 5.2.4. *If $P \nmid m$, $a \in A$, then $P \mid \Phi_m(a)$ if and only if the Carlitz order of $a \pmod{P}$ is m .*

Proof. For $a \in A$, we have $\Phi_m(a) \in A$, this follows from proposition 5.2.6 proved later on. Suppose P divides $\Phi_m(a)$, by proposition 5.2.1, we have $\phi_m(a) \equiv 0 \pmod{P}$. If b is the Carlitz order of $a \pmod{P}$, then b divides m . Suppose $\deg(b) < \deg(m)$, then as above, we get $0 \equiv \phi_b(a) \equiv \prod_{d|b} \Phi_d(a) \pmod{P}$. Consequently, $\Phi_{b_0}(a) \equiv 0 \pmod{P}$ for some b_0 , therefore $\phi_m(a) = \Phi_m(a)\Phi_{b_0}(a) \cdot (\text{other factors}) \equiv 0 \pmod{P^2}$. Since P divides $\Phi_m(a)$, we have $\Phi_m(a + P) \equiv \Phi_m(a) \equiv 0 \pmod{P}$ and similarly for $\Phi_{b_0}(a)$, so $\phi_m(a + P) \equiv 0 \pmod{P}$.

Therefore $0 \equiv \phi_m(a + P) \equiv \phi_m(a) + \phi_m(P) \equiv \phi_m(P) \equiv mP \pmod{P^2}$, since $P \nmid m$, this is impossible and so $\deg(b_0) = \deg(m)$ and since b_0 divides m , it suffices to take $b_0 = m$.

Conversely, suppose that $\phi_m(a) \equiv 0 \pmod{P}$, then $\Phi_d(a) \equiv 0 \pmod{P}$ for some d . But if we have $\deg(d) < \deg(m)$, then the Carlitz order of a would be a factor of m since we would have $\phi_d(a) \equiv 0 \pmod{P}$. Therefore, $\Phi_m(a) \equiv 0 \pmod{P}$ and the proof is complete. \square

Proposition 5.2.1 enables us to extensively study properties of Carlitz cyclotomic polynomials. It is on this fact that most of the analytical proofs are based (as shown later). Notice, it further relates $\phi_m(X)$ to its factors $\Phi_d(X)$, where d divides m . Therefore, it can be used as a recursive formula for computing cyclotomic polynomials. In fact, all the computed Carlitz cyclotomic polynomials in this work are based on this. Although this recursive definition works well for lower degree polynomials and small finite fields, it still has a high computation complexity in the sense that it requires a large computation memory.

Proposition 5.2.5. *Let $P \in A$ be a prime polynomial of degree n , then*

$$\Phi_P(X) = X^{r^n-1} + a_{n-1}X^{r^{n-1}-1} + \cdots + a_1X^{r-1} + P,$$

where $a_i \in A$ and P divides a_i for $1 \leq i \leq n-1$ for all i .

We shall give a detailed proof for this proposition in section 5.4.

It is important to note that for any prime P , $\Phi_P(X)$ is a polynomial in X^{r-1} , with integral coefficients and $\Phi_P(X)$ is Eisenstein, thus analogous to $\widehat{\Phi}_p(X) := \Phi_p(X+1) \in \mathbf{Z}[X]$. We have, $\lambda_p \in \Lambda_p \setminus \{0\}$ is analogous to $\zeta_p - 1$ and not ζ_p . It is this analogy that lies at the heart of our discussion when exploring the coefficients for $\Phi_P(X)$ and their Mahler heights.

Proposition 5.2.6. *Let $m \in A^+$, then $\Phi_m(X) \in A[X]$ is monic and irreducible over k .*

Proof. We first prove that $\Phi_m(X) \in A[X]$.

The field extension K_m of k is the splitting field of the separable polynomial $\phi_m(X) \in k[X]$, since it splits this polynomial and is generated as an algebra by a single (primitive m^{th}) root of the polynomial. Since splitting fields are normal, the extension K_m/k is Galois. Any element of the Galois group $\text{Gal}(K_m/k)$, being a field automorphism, must map λ_m to another Λ_m generator. Therefore, since the Galois group permutes the roots of $\Phi_m(X)$, it must fix the coefficients of $\Phi_m(X)$, so by Galois theory, these coefficients are in k . Since the coefficients are integral over k , they must as well be in A and so $\Phi_m(X) \in A[X]$.

Let $f(X)$ be the minimum polynomial of λ_m in $k[X]$. Then $f(X)$ is monic and has integral coefficients as well, since λ_m is integral over A . We will prove that $f(X) = \Phi_m(X)$ by showing that $\Phi_m(X)$ and $f(X)$ have the same roots. We do so via the following claim,

Claim: For any prime $P \nmid m$, and any Λ_m -generator λ_m , if $f(\lambda_m) = 0$, then $f(\phi_P(\lambda_m)) = 0$.

Since $f(\lambda_m) = 0$, and $(m, P) = 1$, any other Λ_m -generator can be obtained by successively applying the P -Carlitz action on λ_m a finite number of times.

To prove this claim, consider the factorisation $\phi_m(X) = f(X)g(X)$ for some $g(X) \in A[X]$. Writing \mathcal{O}_m for the ring of integers of K_m , we treat the factorisation as taking place in the ring $\mathcal{O}_m[X]$ and proceed to mod out both sides of the factorisation by any prime ideal \wp of \mathcal{O}_m lying above PA . Note, $\phi_m(X)$ has no repeated roots modulo \wp , since its derivative $m \neq 0$ is relatively prime to $\phi_m(X)$ modulo \wp . Therefore, if $f(\lambda_m) \equiv 0 \pmod{\wp}$, then $g(\lambda_m) \not\equiv 0 \pmod{\wp}$. Now $g(\phi_P(\lambda_m)) \equiv g(\lambda_m^{r^{\deg(P)}}) \equiv g(\lambda_m)^{r^{\deg(P)}} \equiv \phi_P(g(\lambda_m)) \not\equiv 0 \pmod{\wp}$. This means, $g(\phi_P(\lambda_m))$ cannot be 0 in \mathbf{C}_∞ , because it does not even equal 0 modulo \wp . We also know, $\phi_P(\lambda_m)$ is a root of $\phi_m(X)$, so if it is not a root of g , it must be a root of f . So $f(\phi_P(\lambda_m)) = 0$, as desired. $\Phi_m(X)$ is irreducible over A , and consequently over k . \square

Proposition 5.2.6 implies that, $\Phi_m(X)$ is the minimal polynomial of any of its roots.

Lemma 5.2.7. *Let $d, m \in A^+$, if d divides m , then $\phi_d(X)$ divides $\phi_m(X)$.*

Proof. $d|m$ implies $(\phi_d(X), \phi_m(X)) = \phi_{(d,m)}(X) = \phi_{(d, sd)}(X) = \phi_d(X)$, for some $s \in A$. \square

As a consequence, if d divides m , then $\Lambda_d \subseteq \Lambda_m$, i.e. Λ_d is a sub-module of Λ_m . (chapter 3).

Corollary 5.2.8. *Let $a, f, g \in A^+$, if a divides (f, g) , then $\phi_a(X)$ divides $(\phi_f(X), \phi_g(X))$.*

Proof. Let d be the GCD of f and g , to make it unique assume d is monic. Then, there exists $s, h \in A$ such that $sf + hg = d$. By \mathbf{F}_r -linearity property of the Carlitz polynomial,

$$\phi_d(\tau) = \phi_{sf+hg}(\tau) = (\phi_{sf} + \phi_{hg})(\tau) = (\phi_s\phi_f + \phi_h\phi_g)(\tau) = \phi_s(\tau) \cdot \phi_f(\tau) + \phi_h(\tau) \cdot \phi_g(\tau).$$

$[\cdot]$ is multiplication in $k\{\tau\}$. So $\phi_d(\tau) = (\phi_f(\tau), \phi_g(\tau))$ hence, $\phi_d(X) = (\phi_f(X), \phi_g(X))$ (as the remainders in the right division algorithms for $A\{\tau\}$, $A[X]$ are equal). This also shows that, any common divisor of f and g is necessarily a divisor of $\phi_f(X)$ and $\phi_g(X)$. \square

Theorem 5.2.9. *Let $s \in \mathbf{N}$, $m \in A^+$, and P be a prime, then*

(a)

$$\Phi_{mP^s}(X) = \begin{cases} \Phi_m(\phi_{P^s}(X)), & (m, P) \neq 1 \\ \Phi_{mP}(\phi_{P^{s-1}}(X)), & (m, P) = 1. \end{cases}$$

(b)

$$\Phi_{mP^s}(X) = \begin{cases} \Phi_m(\phi_{P^s}(X)), & (m, P) \neq 1 \\ \frac{\Phi_m(\phi_{P^s}(X))}{\Phi_m(\phi_{P^{s-1}}(X))}, & (m, P) = 1. \end{cases}$$

Proof. We shall proceed in two parts,

(a) Suppose $(m, P) \neq 1$, this means $P \mid m$.

$$\begin{aligned}\Phi_{mP^s}(X) &= \prod_{d \mid mP^s} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \\ &= \Phi_m(\phi_{P^s}(X)) \prod_{d \mid mP^s, d \nmid m} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \\ &= \Phi_m(\phi_{P^s}(X))\end{aligned}$$

since $d \mid mP^s$ and $d \nmid m$ implies $P^2 \mid d$, therefore $\mu(d) = 0$.

Now suppose $P \nmid m$,

$$\begin{aligned}\Phi_{mP^s}(X) &= \prod_{d \mid mP^s} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \\ &= \Phi_{mP}(\phi_{P^{s-1}}(X)) \prod_{d \mid mP^s, d \nmid mP} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \\ &= \Phi_{mP}(\phi_{P^{s-1}}(X)),\end{aligned}$$

again $d \mid mP^s$ and $d \nmid mP$ implies $P^2 \mid d$, therefore $\mu(d) = 0$ and the result follows.

(b) Suppose $P \nmid m$,

$$\begin{aligned}\Phi_{mP^s}(X) &= \prod_{d \mid mP^s} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \\ &= \prod_{d \mid m} \left(\phi_{\frac{mP^s}{d}}(X) \right)^{\mu(d)} \prod_{d \mid m} \left(\phi_{\frac{mP^s}{Pd}}(X) \right)^{\mu(Pd)},\end{aligned}$$

where in the second product, the divisor of mP^s is of form Pd . Otherwise, we have $\mu(P^t d) = 0$ for $t \geq 2$.

$$\begin{aligned}\Phi_{mP^s}(X) &= \Phi_m(\phi_{P^s}(X)) \prod_{d \mid m} \left(\phi_{\frac{mP^s}{Pd}}(X) \right)^{-\mu(d)} \\ &= \frac{\Phi_m(\phi_{P^s}(X))}{\Phi_m(\phi_{P^{s-1}}(X))}.\end{aligned}$$

□

Corollary 5.2.10.

$$\Phi_{P^s}(X) = \frac{\phi_{P^s}(X)}{\phi_{P^{s-1}}(X)}.$$

Theorem 5.2.11. Let $s \in \mathbf{N}$, $m \in A^+$, and P be a prime, then

$$\Phi_{mP^s}(X) \equiv \begin{cases} \Phi_m(X)^{|P|^s} & (\text{mod } P), \quad (m, P) \neq 1 \\ \Phi_m(X)^{\varphi(P^s)} & (\text{mod } P), \quad (m, P) = 1. \end{cases}$$

Proof. Suppose $P \mid m$, then we have

$$\Phi_{mP^s}(X) = \Phi_m(\phi_{P^s}(X)) \equiv \Phi_m(X^{r^{P^s}}) \equiv \Phi_m(X)^{|P|^s} \pmod{P}.$$

Now suppose $(m, P) = 1$, then

$$\Phi_{mP^s}(X) = \frac{\Phi_m(\phi_{P^s}(X))}{\Phi_m(\phi_{P^{s-1}}(X))} \equiv \frac{(\Phi_m(X^{r^{P^s}}))}{(\Phi_m(X^{r^{P^{s-1}}}))} \equiv \frac{(\Phi_m(X))^{|P|^s}}{(\Phi_m(X))^{|P|^{s-1}}} \equiv \Phi_m(X)^{\varphi(P^s)} \pmod{P}.$$

□

If $a \in A/PA$, then, $\phi_{P^s}(a) \equiv a^{|P|^s} \equiv a \pmod{P}$. Moreover, $\phi_{P^{s-1}}(a) \equiv 0 \pmod{P}$. This follows from the fact that $\phi_{P^s}(a) - \phi_1(a) \equiv 0 \pmod{P}$. Also $\Phi_{P^s}(a) \equiv a^{\varphi(P^s)} \equiv 1 \pmod{P}$ if P does not divide a . In particular, $\Phi_P(a) \equiv a^{|P|-1} \equiv 1 \pmod{P}$.

Proposition 5.2.12. *Let $\alpha \in A^*$ and $m \in A^+$, then $\Phi_{\alpha m}(X) = \Phi_m(X)$.*

Proof. Follows from the definition $\Phi_{\alpha m}(X)$. □

Observation 5.2.13 (Non-reciprocity). *For some $m \in A^+$, $\Phi_m(X) \neq X^{\varphi(m)}\Phi_m(X^{-1})$.*

This property demonstrates that, in general the coefficients of $\Phi_m(X)$ are not palindromic. This is because the Carlitz polynomial itself is not reciprocal and therefore not palindromic.

Example 5.2.14. *Let $a = T^2 + T + 1 \in \mathbf{F}_3[T]$, then we have $\Phi_a(X) = X^6 + (2T + 1)X^4 + (T^2 + T + 1)X^2 + T + 2$ (no palindromy). If we now let $a = T(T + 1) \in \mathbf{F}_3[T]$, in this case we have $\Phi_{T(T+1)}(X) = X^4 + TX^2 + 1$, which is palindromic over $\mathbf{F}_3[T]$ but not over $\mathbf{F}_5[T]$. Over $\mathbf{F}_5[T]$, we have $\Phi_{T(T+1)}(X) = X^{16} + (3T + 2)X^{12} + (3T^2 + 4T + 2)X^8 + (T^3 + 2T^2 + 2T)X^4 + 1$.*

It is also worth mentioning that if one constructs Carlitz polynomials using $\phi_T = T\tau^0 - \tau$ as the Carlitz action, all the above properties remain true. In fact, the polynomials are ‘almost the same’. Here the almost the same simply means that the ratios of the successive corresponding non zero coefficients alternates between -1 ($:= r - 1$) and 1 periodically. This property is further transported to the cyclotomic polynomials which also exhibit alternation in the signs. e.g. in $\mathbf{F}_5[T]$, we have $\Phi_{T^2+T+1}^+(X) = X^{20} + 4TX^{16} + T^2X^{12} + 4T^3X^8 + T^4X^4 + T$ and $\Phi_{T^2+T+1}^-(X) = 4X^{20} + 4TX^{16} + 4T^2X^{12} + 4T^3X^8 + 4T^4X^4 + T$ respectively. Here the cyclotomic polynomial $\Phi_a^+(X)$ corresponds to that computed using $\phi_T = \tau + T\tau^0$ and $\Phi_a^-(X)$ corresponds to that obtained when using the isomorphic module $\phi_T = T\tau^0 - \tau$.

Theorem 5.2.15. *Let m_0 be the square free part of m , then $\Phi_m(X) = \Phi_{m_0}(\phi_{\frac{m}{m_0}}(X))$.*

Proof.

$$\Phi_m(X) = \prod_{d \mid m} \phi_{\frac{m}{d}}(X)^{\mu(d)} = \prod_{d \mid m, d \mid m_0} \phi_{\frac{m}{d}}(X)^{\mu(d)} = \prod_{d \mid m_0} \phi_{\frac{m_0}{d}}(\phi_{\frac{m}{m_0}}(X))^{\mu(d)} = \Phi_{m_0}(\phi_{\frac{m}{m_0}}(X)).$$

□

For example, let $m = T^3(T + 1) \in \mathbf{F}_2[T]$, then $m_0 = T(T + 1)$ and $\Phi_{m_0}(X) = X + 1$. We have $\phi_{T^2}(X) = X^4 + (T^2 + T)X^2 + T^2X$ so $\Phi_m(X) = \Phi_{m_0}(\phi_{T^2}(X)) = X^4 + (T^2 + T)X^2 + T^2X + 1$.

5.3 Coefficients of Carlitz cyclotomic polynomials

Our first step towards the study of coefficients, order and height of $\Phi_m(X)$, will be imitation of classical results. We already know that for any $m \in A$, $\phi_m(X)$ and $\Phi_m(X)$ have coefficients belonging to A . Moreover, the derivative of $\phi_m(X)$ is m ; so it is obvious that A is the set of coefficients of $\phi_m(X)$ (unlike $g_n(X)$ whose coefficients are always $-1, 0, 1$). If $P \in A$ is a prime then, from proposition 5.3.20, we have $\Phi_{P^s}(0) = P$ and so all primes in A appear as coefficients in some cyclotomic polynomial. This tempts us to conjecture,

Conjecture 5.3.1. *Every polynomial in A appears as a coefficient in some cyclotomic polynomial.*

The analogue to this conjecture is true in the classical case and was proved by Suzuki in 1987, see theorem 1.3.1. In order to talk about heights, we first investigate the notion of size of coefficients of $\Phi_m(X)$. We shall work with $|\cdot|_{\frac{1}{r}}$, the absolute value corresponding to the place at infinity. In chapter 4, we defined $|f|_{\infty} := |f|_{\frac{1}{r}} = \left(\frac{1}{r}\right)^{v_{\infty}(f)}$ for every $f \in \mathbf{C}_{\infty}$. (much as it is still non-archimedean, it is conventionally analogous to the natural absolute value in \mathbf{Q}). We refer to the associated norm, as the standard norm on \mathbf{C}_{∞} . Moreover, for all $f \in A$, we have $|f|_{\infty} = r^{\deg(f)}$. A polynomial has a large size if its degree is large and vice versa.

With the above notion, we define the height and order of $\Phi_m(X)$ in terms of absolute values in the usual way. However, the problem with this kind of approach is that, all the absolute values in A are non-archimedean and therefore results entirely depend on the underlying field \mathbf{F}_r . However, the non-archimedeanity has a wonderful property in that the height function turns out to be multiplicative and so we are able to calculate the height explicitly.

Definition 5.3.2. *Let $m \in A$, the order of $\Phi_m(X)$, denoted by $\text{ord}_A(m)$ is the number of distinct irreducible factors of m (the subscript shows that $\text{ord}_A(\cdot)$ depends on the base ring).*

We say, $\Phi_m(X)$ is prime if the order of m is 1 e.g. $\Phi_P(X)$ where $P \in A$ is a prime in A ; $\Phi_m(X)$ is binary if it has order 2. Similarly, $\Phi_m(X)$ is ternary if m has 3 distinct prime factors and so on and so forth. We pointed out that, the order of $\Phi_m(X)$ depends on the underlying field (in particular, the ring A). This is because, an element may be irreducible over one ring but reducible over (some or all) the others e.g. the element $f = T^2 + 1$ is irreducible in $\mathbf{F}_3[T]$ but not in $\mathbf{F}_5[T]$. So $\text{ord}_{\mathbf{F}_3[T]}(T^2 + 1) = 2$ and $\text{ord}_{\mathbf{F}_5[T]}(T^2 + 1) = 3$.

Definition 5.3.3. Let $f(X) = \sum_{i=1}^d a_i X^i \in A[X]$, the P -adic height of f relative to $|\cdot|_P$ is defined as $\mathcal{H}_P(f) := \max\{|a_i|_P \text{ for all } i \text{ such that } a_i \neq 0\}$ and the P -adic logarithmic height of f relative to $|\cdot|_P$ is $h_P(f) := \max\{\text{Log}_r(|a_i|_P) \text{ for all } i \text{ such that } a_i \neq 0\} = \text{Log}_r(\mathcal{H}_P(f))$.

In this thesis, unless explicitly stated, we shall assume that $P = \infty$, set $\mathcal{H}(f) := \mathcal{H}_\infty(f)$ and $h := h_\infty$. In this case, $f(X)$ is said to be flat if its logarithmic height is 0 i.e. all its non-zero coefficients are units in A , for example, $f(X) = X^{r^2} + \alpha X^r + \beta$, where $\alpha, \beta \in \mathbf{F}_r$ is flat whereas $g(X) = X^{r^2} + (T^r + T)X^r + \alpha$ is non flat. We will shortly show that the logarithmic height of $\phi_m(X)$ is $r^{\deg(m)-1}$. Unlike the classical case where $\mathcal{H}(n) = \mathcal{H}(n_0)$ with n_0 being the odd square-free part of n ; over A , this fact is in general false. This is because, the height function in non-archimedean analysis is multiplicative as shown by the following lemma.

Lemma 5.3.4 ([17], page 140). Let $\mathcal{H}(f)$ be the height of the polynomial f with respect to a non-archimedean absolute value $|\cdot|$, then $\mathcal{H}(fg) = \mathcal{H}(f)\mathcal{H}(g)$. i.e. the height function with respect to non-archimedean valuation is multiplicative.

Proof. Let $f(x) = a_n x^n + \dots + a_0$ and $g(x) = b_m x^m + \dots + b_0$. Among the coefficients a_n, \dots, a_0 consider those with the maximal absolute value (there can be several such coefficients) and select among them the coefficient a_r and with the greatest index r . Similarly select the coefficient b_s of maximal absolute value and with the greatest index s . Clearly, $(fg)(x) = f(x)g(x) = c_{n+m} x^{m+n} + \dots + c_0$ where $c_k = \sum_{i+j=k} a_i b_j$. Since $|\cdot|$ is a non-archimedean absolute value, we deduce $|c_k| \leq \max_{i+j=k} \{|a_i| \cdot |b_j|\}$. Hence

$$\begin{cases} |c_k| < |a_r| |b_s|, & \text{if } k > r + s, \\ |c_{r+s}| = |a_r| |b_s| (1 + \alpha), & \text{where } |\alpha| < 1, \\ |c_k| \leq |a_r| |b_s|, & \text{if } k < r + s, \end{cases}$$

In non-archimedean analysis $|\alpha| < 1 \Rightarrow |1 + \alpha| = 1$. Observe $|1 + \alpha| \leq \max\{1, |\alpha|\} = 1$ and $1 = |1 + \alpha - \alpha| \leq \max\{|1 + \alpha|, |\alpha|\} \leq |1 + \alpha|$. Therefore $|c_{r+s}| = |a_r| \cdot |b_s|$, and $|c_k| \leq |a_r| \cdot |b_s|$ for $k \neq r + s$. Hence $\mathcal{H}(fg) = |c_{r+s}| = |a_r| \cdot |b_s| = \mathcal{H}(f)\mathcal{H}(g)$. \square

Since all the absolute values over function fields are non-archimedean, we therefore have,

Theorem 5.3.5. Let $a \in A^+$ with $\deg(a) \geq 1$, then $h(\phi_a(X)) = r^{\deg(a)-1}$.

Proof. Let $a \in A^+$ with $\deg(a) = n$, then $\phi_a(X) = \sum_{j=0}^n c_j X^{r^j}$ with $\deg(c_j) = r^j(n - j)$. We also know that if $f \in A$ then $|f|_\infty = r^{\deg(f)}$, so $|c_j|_\infty = r^{r^j(n-j)}$. Consider the real valued function $y = r^x(n - x)$ where r and n are fixed positive integers (with $r \geq 2$). In this case, the maximum value is obtained at $x = n - \frac{1}{\ln r}$. Using this with our integer valued case, we have two possible values either at $x = n$ or $n - 1$, when $r \geq 3$. In this case we have $y = 0$ or $y = r^n$, and clearly the maximum is obtained when $x = n - 1$. In the case where $r = 2$, we have $x = n - 1$ or $n - 2$, and in both cases we obtain $y = 2^{n-1}$, therefore, we can either take $j = n - 1$ or $n - 2$. Hence $h(\phi_a(X)) = \text{Log}_r(|c_{n-1}|_\infty) = r^{n-1}$. \square

Lemma 5.3.6. *Let $P \in A^+$ be a prime, then $h(\phi_P(X)) = h(\Phi_P(X))$.*

Proof. This follows from the following facts, (i) $\phi_P(X) = \Phi_1(X)\Phi_P(X)$, (ii) $h(\Phi_1(X)) = 0$. So we have $h(\phi_P(X)) = \text{Log}_r(\mathcal{H}(\Phi_1(X)\Phi_P(X))) = h(X) + h(\Phi_P(X)) = h(\Phi_P(X))$. \square

Proposition 5.3.7. *Let $P \in A^+$ be a prime of degree n , then $h(\Phi_{P^s}(X)) = r^{ns-n-1}(r^n - 1)$.*

Proof. We have,

$$\mu(P^{s-j}) = \begin{cases} -1, & \text{for } j = s - 1, \\ +1, & \text{for } j = s \\ 0, & \text{otherwise.} \end{cases}$$

So by multiplicativity of \mathcal{H} ,

$$\mathcal{H}(\Phi_{P^s}(X)) = \prod_{j=0}^s \mathcal{H}(\phi_{P^j}(X))^{\mu(P^{s-j})} = \frac{\mathcal{H}(\phi_{P^s}(X))}{\mathcal{H}(\phi_{P^{s-1}}(X))} = \frac{r^{r^{ns-1}}}{r^{r^{ns-1-1}}} = r^{r^{ns-n-1}(r^n-1)},$$

and so $h(\Phi_{P^s}(X)) = r^{ns-n-1}(r^n - 1)$ as required. \square

Theorem 5.3.8. *Given $m \in A^+$, we have*

$$h(\Phi_m(X)) = \sum_{d^+|m} r^{\deg(d^+)-1} \mu\left(\frac{m}{d^+}\right)$$

where d^+ denotes monic factors of m with positive degree.

Proof. $\mathcal{H}(\Phi_m(X)) = \prod_{d|m} \mathcal{H}(\phi_d(X))^{\mu(\frac{m}{d})} = \prod_{d^+|m} r^{\deg(d^+)-1} \mu\left(\frac{m}{d^+}\right) = r^{\sum_{d^+|m} r^{\deg(d^+)-1} \mu\left(\frac{m}{d^+}\right)}$. Here, d^+ denotes divisors of m with positive degree. Constant polynomial divisors contribute nothing since the height of their corresponding Carlitz polynomials is 1. The proof is completed by taking the logarithms to the base r on both ends of the above relation. \square

Corollary 5.3.9. *Let $m = P_1^{s_1} P_2^{s_2}$ where P_1 and P_2 are two distinct primes in A of degree n_1 and n_2 resp., then $h(\Phi_m(X)) = r^{n_1 s_1 + n_2 s_2 - 1} + r^{n_1(s_1-1) + n_2(s_2-1) - 1} - r^{n_1(s_1-1) + n_2 s_2 - 1} - r^{n_1 s_1 + n_2(s_2-1) - 1}$.*

Proof. Since $m = P_1^{s_1} P_2^{s_2}$, we have

$$h(\Phi_m(X)) = \sum_{d|m} h(\phi_d(X)) \mu\left(\frac{m}{d}\right) = \sum_{d^+|m} r^{\deg(d^+)-1} \mu\left(\frac{m}{d^+}\right) = \sum_{d^+|m} r^{\deg(d^+)-1} \mu\left(\frac{m}{d^+}\right).$$

The only factors d that contribute non-zero terms in the sum are $P_1^{s_1} P_2^{s_2}$, $P_1^{s_1-1} P_2^{s_2}$, $P_1^{s_1} P_2^{s_2-1}$ and $P_1^{s_1-1} P_2^{s_2-1}$. For otherwise we have $\mu\left(\frac{m}{d}\right) = 0$, hence

$$h(\Phi_m(X)) = r^{n_1 s_1 + n_2 s_2 - 1} + r^{n_1(s_1-1) + n_2(s_2-1) - 1} - r^{n_1(s_1-1) + n_2 s_2 - 1} - r^{n_1 s_1 + n_2(s_2-1) - 1}.$$

\square

For-example, if we work over $\mathbf{F}_3[T]$, taking $P_1 = T^2 + 1$, $P_2 = T^2 + 2T + 2$ for our primes, and setting $m = P_1^2 P_2$. Our brute force algorithm using **SAGE** returns the logarithmic height of $\Phi_m(X)$ as 192. Writing this polynomial explicitly would require another 15 pages of the thesis. With the above formula, we can compute this value quickly without worrying about the involved “monster polynomials”. We have $n_1 = n_2 = s_1 = 2$, $s_2 = 1$, $r = 3$. So

$$\begin{aligned} h(\Phi_m(X)) &= r^{n_1 s_1 + n_2 s_2 - 1} + r^{n_1(s_1 - 1) + n_2(s_2 - 1) - 1} - r^{n_1(s_1 - 1) + n_2 s_2 - 1} - r^{n_1 s_1 + n_2(s_2 - 1) - 1} \\ &= 3^{2(2) + 2(1) - 1} + 3^{2(2-1) + 2(1-1) - 1} - 3^{2(2-1) + 2(1) - 1} - 3^{2(2) + 2(1-1) - 1} = 192. \end{aligned}$$

By the above results, we are unable to classify Carlitz cyclotomic polynomials according to height depending on order (as in the classical case). The classical result in all order 1 and 2 cyclotomic polynomials being flat is totally lost. However, we can confidently say that the height of $\Phi_m(X)$ over A is a power of r and is unbounded from above. In the next theorem, we explicitly determine the coefficient of $\phi_m(X)$ with the largest size.

Theorem 5.3.10. *Let $m \in A^+$, $\deg(m) = n$, and ϑ_m be the coefficient of maximum size in $\phi_m(X)$, then $\vartheta_m = (\tau^{n-1} + \dots + \tau^0)(T) + m_1$, where m_1 is the coefficient of T^{n-1} in m .*

Proof. Suppose $\phi_{T^n}(X) = \sum_{i=0}^n a_i X^i$, then by theorem 5.3.5 and lemma 4.3.6, we must have $\vartheta_{T^n} = a_{n-1} = \frac{a_{n-2} - a_{n-2}}{T^{n-1} - T}$. Moreover, $a_n = 1$ since T^n is monic, so $T^n - T = a_{n-1}^r - a_{n-1}$ and therefore, we obtain $(\tau^n - \tau^0)(T) = (\tau - \tau^0)(a_{n-1})$. Using the left division algorithm, we obtain $a_{n-1} = (\tau^{n-1} + \dots + \tau^0)(T)$. Next we have $(a_{n-1})(\tau^{n-1} - \tau^0)(T) = (\tau - \tau^0)(a_{n-2})$ and so $a_{n-2} = (\tau - \tau^0)^{-1}(a_{n-1})(\tau^{n-1} - \tau^0)(T)$. In general, one obtains the following recursion formula $a_{n-j} = (\tau - \tau^0)^{-1}(a_{n-j+1})(\tau^{n-j+1} - \tau^0)(T)$ for $n \geq 1$. This formula gives coefficients of $\phi_{T^n}(X)$ in descending order. The term of maximum size in $\phi_{T^n}(X)$ is $(T^{r^{n-1}} + \dots + T)X^{r^{n-1}}$, similarly $\vartheta_{T^{n-1}} = (T^{r^{n-2}} + \dots + T)X^{r^{n-2}}$. If we let $\phi_m(X) = \sum_{i=0}^n b_i X^i$, since ϕ is a ring homomorphism, we have $b_{n-1} = (\tau^{n-1} + \dots + \tau^0)(T) + m_1$, where the m_1 is the coefficient of T^{n-1} in m . This arises from the fact $\phi_{T^{n-1}}(X) = m_1 X^{r^{n-1}} + \dots + T^{n-1} X$ is the only lower degree Carlitz polynomial linked to m with a term of the form $[]X^{r^{n-1}}$. \square

It is an obvious non-analogy with the classical cyclotomic polynomials; that none of the Carlitz cyclotomic polynomials (with the exception of $\Phi_{T(T+1)}(X) = X + 1$ in $\mathbf{F}_2[T]$) are flat. In order to get the analogy right, we have to look at these polynomials more closely. We know that $\Phi_P(X)$ has order one and is Eisenstein at the prime P , so we need to consider Eisenstein forms of order one classical cyclotomic polynomials. For details about this consideration and its results, refer to Appendix 8.1.

Definition 5.3.11. *Let $\Phi_m(X)$ be an order one Carlitz cyclotomic polynomial, the prime height of $\Phi_m(X)$ is $\mathcal{A}(m) := h_P(\Phi_m(X))$, where P is the unique prime factor of m .*

Theorem 5.3.12. *For all primes $P \in A^+$, we have $\mathcal{A}(P) = 1$.*

Proof. Suppose $\deg(P) = 1$ (P is of the form $T + \alpha$ where $\alpha \in \mathbf{F}_r$), then $\Phi_P(X) = X^{r-1} + P$, clearly its valuation set is $V_P = \{0, 1\}$, therefore $\mathcal{A}(P) = 1$. Suppose P has degree $n > 1$, then applying lemma 4.3.6, we have $\Phi_P(X) = a_0 + a_1 X^{r-1} + \dots + a_n X^{r^n-1}$, where the coefficients are given by;

$$a_0 = P, a_1 = \frac{a_0^r - a_0}{T^r - T}, a_2 = \frac{a_1^r - a_1}{T^{r^2} - T}, \dots, a_{n-1} = \frac{a_{n-2}^r - a_{n-2}}{T^{r^{n-1}} - T}, a_n = 1.$$

Observe that $v_P(a_0) = 1$ and $v_P(a_n) = 0$. Now, $v_P(a_0^r - a_0) = v_P(P^r - P) = 1$ since P does not divide $(P^{r-1} - 1)$ and $v_P(T^r - T) = 0$ since $\deg(P) > 1$, hence $v_P(a_1) = 1$. Similarly, $v_P(a_2) = v(a_1^r - a_1) - v_P(T^{r^2} - T) = 1$. This can be done until a_{n-1} is reached, because if $\deg(P) = n$, then P divides $T^{r^n} - T$ but not $T^{r^m} - T$ for $m < n$. Therefore, we have $v_P(a_n) = v_P(a_n^r - a_{n-1}) - v_P(T^{r^n} - T) = 0$, because at this point, at-least one of the factors of $T^{r^n} - T$ is P . Therefore, the valuation set of $\Phi_P(X)$ is $V_P = \{0, 1\}$ hence $\mathcal{A}(P) = 1$. \square

We now attempt to investigate what happens to the prime height for higher powers of P .

Lemma 5.3.13. *Let $\eta_\alpha : k \rightarrow k$ be the map $\eta_\alpha(f) = f(T + \alpha)$, where $f \in A$, $\alpha \in \mathbf{F}_r$. Then we have $\Phi_{(T+\alpha)^s}(X) = \eta_\alpha(\Phi_{T^s}(X))$.*

Proof. Now η_α is an \mathbf{F}_r -homomorphism, it fixes \mathbf{F}_r and permutes the elements of A . We also have $\eta_0(f) = f$ for all $f \in A$, and $\eta_\alpha(fg) = (f \cdot g)(T + \alpha) = f(T + \alpha)g(T + \alpha) = \eta_\alpha(f)\eta_\alpha(g)$. By theorem 5.2.9, $\Phi_{(T+\alpha)^s}(X) = \Phi_{T+\alpha}(\phi_{(T+\alpha)^{s-1}}(X)) = \phi_{(T+\alpha)^{s-1}}(X)^{r-1} + T + \alpha$. Similarly, $\Phi_{T^s}(X) = \Phi_T(\phi_{T^{s-1}}(X)) = \phi_{T^{s-1}}(X)^{r-1} + T$. Left to know the action of η_α on $\phi_{T^{s-1}}(X)$. But since η is both an \mathbf{F}_r -homomorphism and an A -ring homomorphism, we then have $\eta(\Phi_{T^s}(X)) = \eta(\phi_{T^{s-1}}(X)^{r-1} + T) = \phi_{(T+\alpha)^{s-1}}(X)^{r-1} + T + \alpha = \Phi_{(T+\alpha)^s}(X)$. \square

Theorem 5.3.14. $\Phi_{\eta_\alpha(m)}(X) = \eta_\alpha(\Phi_m(X))$ for any $m \in A^+$.

Proof. Let $\phi_m(X) = \sum_{j=0}^n a_j X^{r^j}$ and $\phi_{\eta_\alpha(m)}(X) = \sum_{j=0}^n b_j X^{r^j}$. Without loss of generality, assume m is monic. Since η_α is a ring homomorphism, we have $\eta_\alpha(a_0) = \eta_\alpha(m) = b_0$ and $\eta_\alpha(a_n) = \eta_\alpha(1) = 1 = b_n$. This is true since m and $\eta_\alpha(m)$ are both monic. For $1 \leq j < n$,

$$\eta_\alpha(a_j) = \eta_\alpha\left(\frac{a_{j-1}^r - a_{j-1}}{T^{r^j} - T}\right) = \frac{(\eta_\alpha(a_{j-1}))^r - \eta_\alpha(a_{j-1})}{(T+\alpha)^{r^j} - (T+\alpha)} = \frac{(\eta_\alpha(a_{j-1}))^r - \eta_\alpha(a_{j-1})}{T^{r^j} - T} = b_j$$

and so $\eta_\alpha(\phi_m(X)) = \sum_{j=0}^n \eta_\alpha(a_j) X^{r^j} = \sum_{j=0}^n b_j X^{r^j} = \phi_{\eta_\alpha(m)}(X)$. Now we obtain,

$$\begin{aligned} \eta_\alpha(\Phi_m(X)) &= \prod_{d|m} \eta_\alpha(\phi_d(X)^{\mu(\frac{m}{d})}) = \prod_{d|m} \eta_\alpha(\phi_d(X))^{\mu(\frac{m}{d})} = \prod_{d|m} (\phi_{\eta_\alpha(d)}(X))^{\mu(\frac{m}{d})} \\ &= \prod_{\eta_\alpha(d)|\eta_\alpha(m)} (\phi_{\eta_\alpha(d)}(X))^{\mu(\frac{\eta_\alpha(m)}{\eta_\alpha(d)})} = \Phi_{\eta_\alpha(m)}(X). \end{aligned}$$

\square

Example 5.3.15. *Let $m_1 = T^3 + T + 1 \in \mathbf{F}_2[T]$, we have $\Phi_{m_1}(X) = X^7 + (T^4 + T^2 + T)X^3 + (T^4 + T^3 + T^2 + 1)X + T^3 + T + 1$. There is another prime in $\mathbf{F}_2[T]$ of degree 3 given by $m_2 =$*

$T^3 + T^2 + 1$. A straight forward computation shows that, $m_2 = \eta_1(m_1)$ and;

$$\eta_1(\Phi_{m_1}(X)) = X^7 + (T^4 + T^2 + T + 1)X^3 + (T^4 + T^3 + T)X + T^3 + T^2 + 1 = \Phi_{m_2}(X).$$

Theorem 5.3.16. Let $P \in A^+$ be prime of degree n , $s \in \mathbf{N}_{\geq 2}$, then $\mathcal{A}(P^s) = (r^n - 1)(s - 1)$.

Before we prove this theorem, we need the following lemma.

Lemma 5.3.17. Let $s \in \mathbf{N}$ and P be a prime of degree n in A . The coefficients of X^{r^j} for $0 \leq j < n$ in $\phi_{P^s}(X)$ have maximum valuation with respect to P . Moreover $\mathcal{A}(\phi_{P^s}(X)) = s$.

Proof. $\mathcal{A}(\phi_P(X)) = \mathcal{A}(\Phi_1(X)\Phi_P(X)) = 0 + 1 = 1$ by theorem 5.3.12. Assume $s \geq 2$, and $\phi_{P^s}(X) = \sum_{j=0}^{ns} a_j X^{r^j}$. We know recursively; $a_j = \frac{a_{j-1}^{r-1} - a_{j-1}}{T^{r^j} - T}$ for $1 \leq j \leq ns$ and $a_0 = P^s$. It is obvious $v_P(a_0) = s$ and $v_P(a_{ns}) = 0$. Left to show is; $0 < v_P(a_j) \leq s$ for $0 \leq j < ns$. Now, we have $v_P(a_j) = v_P(a_{j-1}) + v_P(a_{j-1}^{r-1} - 1) - v_P(T^{r^j} - T)$ for $1 \leq j \leq ns$. Since P divides a_j , we must have $v_P(a_{j-1}^{r-1} - 1) = 0$ and so $v_P(a_j) - v_P(a_{j-1}) = -v_P(T^{r^j} - T)$. From the theory of finite fields, $v_P(T^{r^j} - T) = 0$ for $j \not\equiv 0 \pmod{n}$ and $v_P(T^{r^{tn}} - T) = 1$ for any $t \in \mathbf{Z}^+$. We obtain a telescoping sum that adds up to $v_P(a_j) = s - \sum_{t=1}^j v_P(T^{r^t} - T) = s - \lfloor \frac{j}{n} \rfloor$. \square

This lemma shows that the coefficients of $\phi_{P^s}(X)$ with the highest valuation with respect to P are the coefficients of X^{r^j} with $j = 1, \dots, 2n - 1$ (where in this case $v_P(a_j) = s$ for $j = 1, 2, \dots, n - 1$ and $s - 1$ for $j = n, n + 1, \dots, 2n - 1$) i.e. the upper bound to the prime height of $\phi_{P^s}(X)$ is s . Now, since $\Phi_{P^s}(X)$ is Eisenstein for the prime P , so we have $v_P(\Phi_{P^s}(0)) = 1$ i.e. the prime height of $\Phi_{P^s}(X)$ is always ≥ 1 . This argument, coupled by an induction process on s , we observe that the next suitable candidate for maximum valuation with respect to P is the coefficient of $X^{r^n - 1}$. This comes from the fact v_P is non archimedean. Others may exist, but this is sufficient. We now prove theorem 5.3.16.

Proof. We proceed by induction on powers s of P . Trivially, we have $\Phi_1(X) = X$ and $\Phi_P(X) = X^{r^n - 1} + a_1 X^{r(r^n - 1)} + \dots + a_{r(r^n - 1)} X^{r-1} + P$, where by applying theorem 5.3.12, we obtain $\mathcal{A}(P) = 1$. In particular $v_P(a_{r(r^n - 1)}) = 1$. Since both $\phi_P(X)$ and $\Phi_P(X)$ have each prime height 1, and $r^n - 1 > r^{n-1}$ for all r and $n \in \mathbf{N}$, then it is clear $(\phi_P(X))^{r^n - 1}$ contains the term with the highest valuation with respect to P . So

$$\begin{aligned} \Phi_{P^2}(X) &= \Phi_P(\phi_P(X)) \\ &= (\phi_P(X))^{r^n - 1} + \dots + P \\ &= X^{r^n - 1} \left(\prod_{t=1}^1 \Phi_P(X)^{r^n - 1} \right) + \dots + P. \end{aligned}$$

So the coefficient of $X^{r^n - 1}$ in $\Phi_{P^2}(X)$ is $\prod_{t=1}^1 \Phi_P(0)^{r^n - 1} = P^{r^n - 1}$, so for $s = 2$ we observe that $\mathcal{A}(P^2) = r^n - 1 = (r^n - 1)(2 - 1)$, formula true for $s = 2$. Suppose it is true for $s = n'$,

i.e. $\mathcal{A}(P^{n'}) = (r^{n'} - 1)(s - 1)$. We now compute $\Phi_{P^{n'+1}}(X)$. Now using theorem 5.2.9 and arguing using lemma 5.3.17 (to see position of maximum valuation), we obtain

$$\begin{aligned}\Phi_{P^{n'+1}}(X) &= \Phi_P(\phi_{P^{n'}}(X)) \\ &= \phi_{P^{n'}}(X)^{r^n-1} + \dots + P \\ &= X^{r^n-1} \left(\prod_{t=1}^{n'} \Phi_{P^t}(X)^{r^n-1} \right) + \dots + P,\end{aligned}$$

with the position having maximum valuation (with respect to P) at X^{r^n-1} . To obtain the coefficient of X^{r^n-1} , consider the constant terms of $\Phi_{P^t}(X)$. So the coefficient of X^{r^n-1} in $\Phi_{P^{n'+1}}(X)$ is $\prod_{t=1}^{n'} \Phi_{P^t}(0)^{r^n-1} = P^{n'(r^n-1)}$ and so $\mathcal{A}(P^{n'+1}) = (r^n - 1)(n' + 1 - 1)$. \square

So we obtain $\mathcal{A}(P^s) \propto s - 1$. This parallels the classical results where $\mathcal{A}(p^s) \propto s$.

Example 5.3.18. Suppose $A = \mathbf{F}_3[T]$, and $P = T \in A$. Computations using SAGE yield $\Phi_{T^4}(x) = x^{54} + (2T^9 + 2T^3 + 2T)x^{36} + (2T^6 + 2T^4 + 2T^2)x^{30} + 2T^3x^{28} + (T^{18} + 2T^{12} + 2T^{10} + T^6 + 2T^4 + T^2)x^{18} + (2T^{15} + 2T^{13} + 2T^{11} + 2T^9 + T^7 + T^5 + 2T^3)x^{12} + (2T^{12} + 2T^6 + 2T^4)x^{10} + (T^{12} + 2T^{10} + 2T^6 + T^4)x^6 + (2T^9 + 2T^7 + 2T^5)x^4 + T^6x^2 + T$. The coefficient with highest valuation with respect to the prime T is T^6 and so $\mathcal{A}(P^4) = 6 = (3^1 - 1)(4 - 1)$.

Proposition 5.3.19. Let $P \in \mathbf{F}_2[T]$ be a non-linear prime, $\alpha \in \mathbf{F}_2$, then $\mathcal{H}_P((T + \alpha)P) = 1$.

Proof. It suffices to show that all the coefficients of $\Phi_{(T+\alpha)P}(X)$ are $\not\equiv 0 \pmod{P}$. It is sufficient to work with $\Phi_T(X)$, so from proposition 5.3.20, we have the following equation $\Phi_T(X)\Phi_{TQ}(X) = \phi_Q(X) + T \equiv X^{2^n} + T \pmod{Q}$, where $Q = \eta_\alpha(P)$ (by lemma 4.3.6 and theorem 5.2.9). Since P is a non linear polynomial, so is Q , we must have $n \geq 2$ and that $\Phi_{TQ}(X) \equiv X^{2^n-1} + a_1X^{2^n-2} + \dots + a_{2^n-2}X + 1 \pmod{Q}$ with all the terms a_i being non-zero (via long division) and having degree $\leq n$, therefore $\mathcal{A}(TQ) = 0$. \square

Let us investigate the case $P = T$. By theorem 5.3.16, $\mathcal{A}(T^2) = r - 1$. This can also be deduced from the following calculation,

$$\begin{aligned}\Phi_{T^2}(X) &= (X^r + TX)^{r-1} + T \\ &= T + \sum_{i=0}^{r-1} \binom{r-1}{i} X^{(r-1)(i+1)} T^{r-1-i} \\ &= T + \sum_{i=0}^{r-1} a_i X^{(r-1)(i+1)} T^{r-1-i}.\end{aligned}$$

The highest possible term in T is T^{r-1} , hence $\mathcal{A}(T^2) = r - 1$.

We now discuss the constant and the middle coefficient of $\Phi_m(X)$. We also give a short proof to a special case of Dirichlet's theorem on primes in an arithmetic progression.

Proposition 5.3.20. *Let $s \in \mathbf{N}$, $m \in A^+$ and P be a prime in A , then*

$$\Phi_m(0) = \begin{cases} 1, & m \neq P^s \\ P, & m = P^s. \end{cases}$$

Proof. We shall proceed in 3 steps. Let $\phi_m(X) = \sum_{i=0}^{|m|} c_m(i)X^i$ and $\Phi_m(X) = \sum_{i=0}^{\phi(m)} a_m(i)X^i$.

1. Let $m = P^s$, then by theorem 5.2.10, $\Phi_{P^s}(X)\phi_{P^{s-1}}(X) = \phi_{P^s}(X)$. We get the constant term of $\Phi_{P^s}(X)$ by solving $a_{P^s}(0)c_{P^{s-1}}(1) = c_{P^s}(1)$, therefore $a_{P^s}(0)P^{s-1} = P^s$.
2. Suppose $m \neq P^s$, we shall proceed by induction on the order of $\Phi_m(X)$ with the help of proposition 5.2.1. Suppose $\Phi_m(X)$ is binary, set $m = PQ$, where P, Q are distinct primes. Then $c_{PQ}(1) = \prod_{d|PQ} a_d(0)$ and $PQ = 1 \cdot P \cdot Q \cdot a_{PQ}(0)$ hence $a_{PQ}(0) = 1$. In general, for $s_1, s_2 \in \mathbf{N}$, if $m = P^{s_1}Q^{s_2}$, by part 1, we get $a_{P^{s_1}Q^{s_2}}(0) = 1$.
3. Suppose the statement is true for orders $s < n$, and $\text{ord}_A(m) = n$. We shall first consider the case for m , square free of order n . We have $c_m(1) = \prod_{d|m} a_d(0)$, therefore by the induction hypothesis we get,

$$m = c_m(1) = a_m(0) \prod_{d|m, d \neq m} a_d(0) = a_m(0) \left(\prod_{Q|m, \text{ a prime}} a_Q(0) \right) \cdot 1 = a_m(0) \cdot m \cdot 1,$$

implying $a_m(0) = 1$. With this construction, if m not square free, then by parts 1, 2, and the first part of 3 we have have $a_m(0) = 1$ which completes the proof.

In fact the same results hold for the classical case. □

Corollary 5.3.21. *Let $a \in A$ and $P \nmid m$, then P divides $\Phi_m(a)$ if and only if $P \equiv 1 \pmod{m}$.*

Proof. Let P be a prime factor of $\Phi_m(a)$, such that P does not divide m . Then we have $P \nmid a$ for otherwise we would have $\Phi_m(a) \equiv 0 \pmod{P}$, and on the other hand we would have $\Phi_m(a) \equiv 1 \pmod{P}$ (when m is product of more than one primes different from P) or $\Phi_m(a) \equiv P_0 \pmod{P}$ (when m is a power of P_0) which is different from zero modulo P unless when P divides m . Either way we have a contradiction. Let f be the Carlitz order of a modulo P , that is to say $\phi_f(a) \equiv 0 \pmod{P}$ for some $0 \neq f \in A/PA$ of least degree. Therefore, f divides m since $\phi_m(a) = 0$. There are two cases we need to consider,

1. If $f = m$, then m divides $P - 1$ since $\phi_{P-1}(a) = \phi_P(a) - \phi_1(a) = a - a \equiv 0 \pmod{P}$.
2. If $0 \leq \deg(f) < \deg(m)$, since $0 \equiv \phi_f(a) = \prod_{d|f} \Phi_d(a) \pmod{P}$, there exists a divisor d of f so that P divides $\Phi_d(a)$. But $d \mid f \mid m$ and $\deg(d) < \deg(m)$, so $\phi_m(X)$ has a repeated root modulo P by proposition 5.2.2 and so P divides m .

(\Leftarrow) Suppose $P \equiv 1 \pmod{m}$, then P does not divide m , and there is an element $a \pmod{P}$ of order m . So $\phi_m(a) = \prod_{d|m} \Phi_d(a) \equiv 0 \pmod{P}$ and the order of a imply that P divides $\Phi_m(a)$. So $P \nmid m$, then P divides $\Phi_m(a)$ for some $a \in A$ if and only if $P \equiv 1 \pmod{m}$. □

For example, over $\mathbf{F}_2[T]$, if we take $a = 1$, $b = T^2 + T$ and $m = T^2 + T$. We have already seen that $\Phi_m(X) = X + 1$, so $\Phi_m(a) = 0$ and $\Phi_m(b) = T^2 + T + 1$. Now $P = T^2 + T + 1$ divides $\Phi_m(T^2 + T + 1)$ but does not divide m , moreover $P \equiv 1 \pmod{m}$. Similarly, take $c = T^6 + T^5 + T^4 + T^3$, then $P_1 = T^2 + T + 1$ and $P_2 = T^4 + T + 1$ are all congruent to 1 modulo m and both divide $\Phi_m(c)$. Another good example is to consider $m = T^2 + T \in \mathbf{F}_3[T]$. Here $\Phi_m(X) = X^4 + (T + 2)X^2 + 1$; now setting $a = T + 2$, we obtain $\Phi_m(a) = T^4 + 2T + 1 = (T + 1)(T^3 + 2T^2 + T + 1)$. Observe that the prime $Q_1 = T + 1$ divides m (so by the corollary is not considered), but $Q_2 = T^3 + 2T^2 + T + 1$ divides $\Phi_m(a)$ and does not divide m . Moreover, $Q_2 \equiv 1 \pmod{m}$, which agrees with corollary 5.3.21.

Proposition 5.3.22 (Special case of Dirichlet’s theorem). *For each $m \in A$ with $\deg(m) > 1$, there are infinitely many primes P with the property that $P \equiv 1 \pmod{m}$.*

Proof. Suppose there are only finitely many primes P_1, \dots, P_s of the form $P_i \equiv 1 \pmod{m}$ for $i = 1, \dots, s$. Let $M = mP_1 \cdots P_s$ and $N \in A$, then

$$\Phi_m(NM) \equiv \begin{cases} 1 \pmod{m}, & \text{if } m \neq P^s, \\ P \pmod{m}, & \text{if } m = P^s \end{cases}.$$

where P is a prime in A . In particular, $\Phi_m(NM)$ is not divisible by P_i and none of its factors (with the exception of P) divides m . This is because, $\Phi_m(NM) \equiv 1 \pmod{P_i}$, otherwise, we would have $\Phi_m(NM) \equiv 0 \pmod{P_i}$ which contradicts $P_i \equiv 1 \pmod{m}$. As $\deg(N) \rightarrow \infty$, we have $\deg(\Phi_m(NM)) \rightarrow \infty$. So for sufficiently large degree of N , we have $\Phi_m(NM) \neq 1$ (by degree comparisons); so there is a prime P_0 that divides $\Phi_m(NM)$. By corollary 5.3.21, $P_0 \equiv 1 \pmod{m}$ and from the above argument, we must have $P_0 \neq P_i$ for $1 \leq i \leq s$. We have just obtained a new prime $P_0 \equiv 1 \pmod{m}$, a contradiction. \square

In the next section, we discuss the analogue of classical cyclotomic extensions.

5.4 Cyclotomic function fields

Like its classical counter-part, the m^{th} Carlitz cyclotomic extension field K_m is obtained by adjoining λ_m , a generator of Λ_m to k , so $K_m = k(\lambda_m)$. We have already seen that K_m/k is Galois with Galois group $\text{Gal}(K_m/k)$. If $\sigma \in \text{Gal}(K_m/k)$, then $\sigma(\lambda_m) = \phi_a(\lambda_m)$ where $(a, m) = 1$ and is determined modulo m i.e. $a \in (A/mA)^*$. This also gives rise to a monomorphism $\theta : \text{Gal}(K_m/k) \hookrightarrow (A/mA)^*$. Irreducibility of $\Phi_m(X)$ (by Proposition 5.2.6), implies that θ is in fact an epimorphism from $\text{Gal}(K_m/k)$ to $(A/mA)^*$, therefore we have established the isomorphism $\text{Gal}(K_m/k) \cong (A/mA)^*$. This implies K_m/k is an abelian extension of k with degree $\varphi(m)$, where $\varphi(m)$ is the Euler totient function. We shall denote the integral closure of A in K_m by $\mathcal{O}_m = A[\lambda_m]$. Our goal is to imitate deductions of classical theory, however

before we do this, we need to study the group of units in \mathcal{O}_m . We begin with the following proposition which also suggests that it suffices to consider only monic polynomials.

Proposition 5.4.1. *Let $0 \neq m_1, m_2 \in A$, then $K_{m_2} = K_{m_1}$ if and only if $m_2 = \alpha m_1$ where $\alpha \in A^*$.*

Proof. (\Leftarrow) $m_2 = \alpha m_1$ with $\alpha \in A^*$, then $\phi_{m_2}(X) = \alpha \phi_{m_1}(X)$, $\Lambda_{m_2} = \Lambda_{m_1} \Rightarrow K_{m_2} = K_{m_1}$. (\Rightarrow) Conversely, suppose $K_{m_2} = K_{m_1}$, we compute the largest torsion sub-module of K_{m_1} . If $\Lambda_m \subseteq K_{m_1}$, then $K_m \subseteq K_{m_1}$, so $\varphi(m) \leq \varphi(m_1)$, for any degree of $m \in A$. So there exists Λ_m such that $\Lambda_m \subseteq \Lambda_{m_1}$, which implies m divides m_1 and $K_m = K_{m_1}$. Let us write $m_1 = ms$, so $\varphi(m_1) = \varphi(m)\varphi(s) \frac{|d|}{\varphi(d)} \geq \varphi(m)\varphi(s)$, where $d = (m, s)$. Since $K_m = K_{m_1}$, and so we have $\varphi(m) = \varphi(m_1)$ therefore $\varphi(s) = 1$. This shows $s \in A^*$, so m_1 is a scalar multiple of m , and so $\Lambda_m = \Lambda_{m_1}$. Therefore, $K_{m_2} = K_{m_1}$, and $\Lambda_{m_2} = \Lambda_{m_1}$. So $m_2 = \alpha m_1$ for some $\alpha \in A^*$. \square

Proposition 5.4.2. *Let λ_m be a Λ_m -generator and suppose, $a \in A$ is co-prime to m . Then $\frac{\phi_a(\lambda_m)}{\lambda_m}$ is a unit in \mathcal{O}_m . Moreover, if m is of order ≥ 2 , then λ_m is itself a unit.*

Proof. ([18], Proposition 12.6) Clearly, since $\phi_m(X) \in A[X]$, is monic and $\phi_m(\lambda_m) = 0$, λ_m is integral over A . Replacing m by a , and substituting $X = \lambda_m$, we see that $\frac{\phi_a(\lambda_m)}{\lambda_m} \in \mathcal{O}_m$ (deduced from 5.2.1). We are required to show that, the reciprocal of this element is in \mathcal{O}_m .

Let $b \in A$ be such that $ba = 1 \pmod{m}$. Then, there exists $f \in A$ such that $ba = 1 + fm$ and we have $\phi_b \phi_a = \phi_{ba} = 1 + \phi_f \phi_m$. Applying this to λ_m yields $\phi_b(\phi_a(\lambda_m)) = \lambda_m$. Therefore,

$$\frac{\lambda_m}{\phi_a(\lambda_m)} = \frac{\phi_b(\phi_a(\lambda_m))}{\phi_a(\lambda_m)} \in \mathcal{O}_m.$$

To prove the second assertion, we have to show that the norm of λ_m is a non-zero constant. Without loss of generality, we assume m is monic. Suppose $m = m_1 m_2$ where m_1 and m_2 are monic and relatively prime. We take λ_m as a generator of Λ_m . Set $\lambda_{m_1} = \phi_{m_2}(\lambda_m)$, and $\lambda_{m_2} = \phi_{m_1}(\lambda_m)$. Then, λ_{m_i} is a primitive m_i^{th} -torsion point for $i = 1, 2$. For all $a \in A$, $\phi_a(X)$ is divisible by $\Phi_1(X) = X$, i.e. $X^{-1} \phi_a(X) \in A[X]$. Consider the factorization,

$$\lambda_{m_1} = \lambda_m \frac{\phi_{m_2}(\lambda_m)}{\lambda_m}.$$

This shows that, λ_m divides λ_{m_1} , and similarly λ_m divides λ_{m_2} in \mathcal{O}_m . Taking norms from K_m to k shows that the norm of λ_m divides a power of $\mathcal{N}_{K_m/k}(\lambda_{m_i})$ for $i = 1, 2$, that is to say $\mathcal{N}_{K_m/k}(\lambda_m)$ divides $\mathcal{N}_{K_m/k}(\lambda_{m_i})$ for $i = 1, 2$.

To finish the proof, we have to do induction on the number of distinct primes dividing m . Now suppose $m = P^e$, a prime power, then both proposition 5.3.20 and corollary 5.4.4 imply, the norm of λ_{P^e} is P , (generator of Λ_{P^e}). Suppose m is a product of two prime powers $P_1^{e_1}$ and $P_2^{e_2}$. Then, from what we have proven, it follows that the norm of λ_m divides a power of P_1 and a power of P_2 . This implies the norm of λ_m is a non-zero constant (in the sense that it belongs to A) and so λ_m is a unit.

If m is divisible by $t > 2$ distinct primes, set

$$m_1 = P_1^{e_1} \text{ and } m_2 = \prod_{i=2}^t P_i^{e_i},$$

then, by induction, λ_{m_2} is a unit and its norm is a non-zero constant. By what we have proven above, it follows that the norm of λ_m is still a non-zero constant. Therefore, λ_m is a unit. \square

If $m = P^e$, then λ is analogous to $\zeta - 1$ in the classical case. Otherwise, $\lambda \in \mathcal{O}_m^*$.

In chapter 1, we intentionally left out details on ramification at a prime power, but now we discuss it in rather a generalised fashion. With little strength and the analogies given, one can construct the proofs for the classical case. We begin by considering the case when $m = P^e$ i.e. a power of an irreducible polynomial P of degree n . Since $\Lambda_m \cong A/P^e A$, an element $\lambda_m \in \Lambda_m$ is a Λ_m -generator if and only if $\phi_{P^e}(\lambda) = 0$ and $\phi_{P^{e-1}}(\lambda_m) \neq 0$. Therefore, the generators of Λ_{P^e} are precisely the roots of,

$$\begin{aligned} \Phi_{P^e}(X) &= \frac{\phi_{P^e}(X)}{\phi_{P^{e-1}}(X)} = \frac{\phi_P(\phi_{P^{e-1}}(X))}{\phi_{P^{e-1}}(X)} \\ &= [P, n]\phi_{P^{e-1}}(X)^{r^n-1} + \cdots + [P, 1]\phi_{P^{e-1}}(X)^{r-1} + P. \end{aligned}$$

and $\deg(\Phi_{P^e}(X)) = |P|^{e-1}(r^n - 1) = |P|^{e-1}(|P| - 1) = \varphi(P^e)$ as it should be. We can now investigate ramification in K_m . We shall achieve this via the theorem below.

Proposition 5.4.3. *Let $e \in \mathbf{Z}^+$ and $P \in A$ be a prime of degree n . Then, K_{P^e} is un-ramified at every prime ideal Q with $QA \neq PA$. The prime ideal PA is totally ramified with ramification index $\varphi(P^e)$ and consequently, $[K_{P^e} : k] = \varphi(P^e)$, $\text{Gal}(K_{P^e}/k) \cong (A/P^e A)^*$. Finally, $\lambda \mathcal{O}_{P^e}$, (where λ is any generator of Λ_{P^e}) is the prime ideal lying above PA .*

Proof. ([18], Proposition 12.7). \square

As a corollary, we restate proposition 5.2.5 and provide another proof to this fact.

Corollary 5.4.4. *Let $e \in \mathbf{N}$, P be a prime. Let λ be a generator of Λ_{P^e} and $g(X) \in k[X]$ its irreducible polynomial (over A). Then $g(X)$ is an Eisenstein polynomial at prime P .*

Proof. ([18], Corollary 12.6) We have,

$$g(X) = \prod_{(a,P)=1} (X - \phi_a(\lambda)),$$

where the product is over all generators of Λ_{P^e} . Except for the leading coefficient, which is 1, the coefficients of g are the elementary symmetric functions of the generators of Λ_{P^e} . Proposition 5.4.3 shows these are all in the ideal $\langle \lambda \rangle$. Therefore, all the coefficients of $g(X)$, except the leading coefficient, are in $\langle \lambda \rangle \cap A = PA$. Since the constant term is P , it follows that $g(X)$ is an Eisenstein polynomial at the prime P . \square

Having dealt with the case $m = P^e$, we now pass on to the general case. Consider a non-constant polynomial $m \in A$ with the prime decomposition $m = \alpha P_1^{e_1} \cdots P_t^{e_t}$, $\alpha \in A^*$.

Theorem 5.4.5. $K_m = \bigvee_{i=1}^t K_{P_i^{e_i}}$ and $P_i A$ with $1 \leq i \leq t$ are the only primes in A ramified in \mathcal{O}_m .

Proof. This proof is divided into 2 parts.

1. Define m_i , to be m divided by $P_i^{e_i}$ and let λ_m be a generator of Λ_m as an A -module. It is clear from our previous discussion that $\phi_{m_i}(\lambda_m)$ is a generator of $\Lambda_{P_i^{e_i}}$.
 (\Rightarrow) Define $\lambda_{P_i^{e_i}} := \phi_{m_i}(\lambda_m)$. Clearly, $K_{P_i^{e_i}} = k(\lambda_{P_i^{e_i}}) \subset k(\lambda_m) = K_m$. Therefore, K_m contains the compositum of the fields $K_{P_i^{e_i}}$, for $1 \leq i \leq t$ i.e. $K_m \supseteq \bigvee_{i=1}^t K_{P_i^{e_i}}$. (\Leftarrow) Since the GCD of the set $\{m_i : 1 \leq i \leq t\}$ is just 1, there exist polynomials $a_i \in A$ such that $1 = \sum_{i=1}^t a_i m_i$. It follows that $1 = \sum_{i=1}^t \phi_{a_i} \phi_{m_i}$. Applying this relation to λ_m we obtain $\lambda_m = \sum_{i=1}^t \phi_{a_i}(\lambda_{P_i^{e_i}})$. This shows λ_m is in the compositum of the fields $K_{P_i^{e_i}}$, therefore $K_m \subseteq \bigvee_{i=1}^t K_{P_i^{e_i}}$, hence the proof that $K_m = \bigvee_{i=1}^t K_{P_i^{e_i}}$, the compositum of these fields.
2. If P is a prime element such that $PA \neq P_i A$ for any i , then by proposition 5.4.3, PA is un-ramified in every $K_{P_i^{e_i}}$ and so must be un-ramified in their compositum K_m . On the other hand, $P_i A$ is totally ramified in $K_{P_i^{e_i}}$ by the same proposition. Therefore, all ideals $P_i A$ are ramified in K_m .

□

Corollary 5.4.6. K_m is ramified only at the primes dividing m and possibly at ∞ .

Using the Carlitz action, \bar{k}_∞ can be turned into an A -module in exactly the same way that we turned k into an A -module; namely, if $a \in A$ and $u \in \bar{k}_\infty$, then we define $\sigma_a(u) = \phi_a(u)$. If $m \in A$ has positive degree, we denote the m -torsion points, \bar{k}_∞ by $\hat{\Lambda}[m]$ or simply by $\hat{\Lambda}_m$. Let ι denote a fixed field isomorphism over k from K_m to \bar{k}_∞ . Now since K_m/k is a Galois extension, all the field isomorphisms over k from K_m to \bar{k}_∞ are of the form $\iota \circ \sigma$ with $\sigma \in \text{Gal}(K_m/k)$. The isomorphism ι corresponds to a prime \wp_∞ of K_m lying over ∞ . To see this, we let $\mathcal{O}_{\wp_\infty} = \{\omega \in K_m : v_\infty(\iota\omega) \geq 0\}$, it is easy to see that \mathcal{O}_{\wp_∞} is a discrete valuation ring inside K_m which contains \mathbf{F}_r and has K_m as its quotient field. By definition, $\mathcal{O}_{\wp_\infty} \setminus \mathbf{F}_r^*$ is a prime of K_m denoted by \wp_∞ , its maximal ideal. The proof of the fact that \wp_∞ lies above ∞ follows immediately. Suppose λ is a root to $\phi_m(X)$ in \bar{k} , since $\phi_m(\lambda) = 0$ implies $\phi_m(\iota\lambda) = \iota(\phi_m(\lambda)) = 0$; ι maps Λ_m to $\hat{\Lambda}_m$. This map is an A -module isomorphism thus, there is $\hat{\lambda}_m \in \hat{\Lambda}_m$ with $v_\infty(\hat{\lambda}) = n - 1 - \frac{1}{r-1}$. Let $\hat{\lambda}_m \in \hat{\Lambda}_m$ be such that $\iota\lambda = \hat{\lambda}_m$.

Let $\mathcal{I} = \{\sigma_\alpha \in \text{Gal}(K_m/k) : \alpha \in \mathbf{F}_r^*\}$ and set K_m^+ , equal to the fixed field of \mathcal{I} . Then ∞ splits completely in K_m^+ and every prime above ∞ in K_m^+ is totally and tamely ramified in K_m . For the proof of this fact is in ([18], Theorem 12.14).

If $f_m(X) = f_{\min}^{\hat{\lambda}}(X) \in k[X]$, then $K_m^+ = k(\hat{\lambda}) \cong k[X]/(f_m(X))k[X]$. Moreover, for $0 \neq m \in A$, K_m/k is a geometric extension i.e. the constant field of K_m is \mathbf{F}_r .

The properties of K_m^+ are so similar to those of \mathbf{Q}^+ in the number field case. We call K_m^+ , the maximal real sub-field of K_m . The motivation for is that, the prime at infinity of k splits completely in K_m^+ and every prime above it (∞) in K_m^+ totally ramifies in K_m . This is analogous to the behaviour of ∞ , the only archimedean prime at infinity of \mathbf{Q} . This splits completely in \mathbf{Q}_n^+ and every prime above it is totally ramified in \mathbf{Q}_n . Also notice that the Galois group of K_m/K_m^+ is isomorphic to \mathbf{F}_r^* , the non-zero units of A , whereas the Galois group of $\mathbf{Q}_n/\mathbf{Q}_n^+$ is isomorphic to $\mathbf{Z}^* = \{\pm 1\}$, still the units of \mathbf{Z} .

In general, we call a finite extension \mathcal{F} of k real if P_∞ splits completely in \mathcal{F} . For example, the theory of quadratic function fields is divided up into the theory of real quadratic function fields, the case where ∞ splits, and complex quadratic function fields, the case where ∞ is either inert or ramifies. It is worth noting; like A and \mathbf{Z} , K_m contains many interesting arithmetic properties analogous to the cyclotomic number field.

We now turn our attention to the middle coefficient of $\Phi_m(X)$. By middle coefficient of $\Phi_m(X)$, we refer to the coefficient of $X^{\frac{\varphi(m)}{2}}$. We have the following proposition.

Proposition 5.4.7. *Let $s, l \in \mathbf{N}$, $m \in \mathbf{F}_r[T]$ where $r \equiv 1 \pmod{2}$ and $P \in A^+$ be a prime. Let $\Phi_m(X) = \sum_{j=0}^{\varphi(m)} a_m(j)X^j$, then the middle coefficient of $\Phi_m(X)$ is*

$$a_m \left(\frac{\varphi(m)}{2} \right) = \begin{cases} 0, & m = P \text{ or } m = (T + \alpha)^l, \\ a_m^+(\frac{s}{2}), & \text{otherwise, } (s = \text{degree of } f_m(X)), \end{cases}$$

where $a_m^+(\frac{s}{2})$ is the middle coefficient of $f_m(X)$, the minimal polynomial of K_m^+ -generators.

Proof. In this proof, we shall consider three cases,

1. Consider $m = T^s, s \in \mathbf{N}$, and $r \neq 2^t$ for all $t \in \mathbf{N}$.

When $m = T^s$, then $\Phi_m(X) = \Phi_T(\phi_{T^{s-1}}(X)) = (\phi_{T^{s-1}}(X))^{r-1} + T$, a polynomial with zero as its middle coefficient. This follows from the fact that $\varphi(T^s) = r^{s-1}(r-1)$, and the observation that there is no term in $\phi_{T^{s-1}}(X)$ with $X^{\frac{r^{s-1}}{2}(r-1)}$. For if it existed (i.e. was there), then we would have 2 divide r^{s-1} , hence $r \equiv 0 \pmod{2}$, which contradicts our assumption. Therefore, we must have $a_m \left(\frac{\varphi(m)}{2} \right) = 0$ and the result follows upon applying the ring homomorphism η_α .

2. Consider $m = P$ with degree n , clearly we know $\Phi_P(X)$ is a polynomial in X^{r-1} and therefore its middle term would correspond to the term in $X^{\frac{r^n-1}{2}} = X^{(r-1)\frac{1+r+\dots+r^{n-1}}{2}}$. But there is no term in $\Phi_P(X)$ with $X^{\frac{r^n-1}{2}}$ since there exists no $n > 1$ such that $\frac{r^n-1}{2} = r-1$. Using theorem 5.3.14, we can extend this to all primes of degree n .

3. Consider m to be a product of more than one distinct primes. We already know, if λ is a generator of Λ_m , then λ is an algebraic unit (by proposition 5.4.2), and so is $\phi_a(\lambda)$ for any $0 \neq a \in A_m$. Now, let $f_m(X)$ be the minimal polynomial of λ^{r-1} , the generator of K_m^+ , the maximal real sub-field of K_m . It is not hard to show using elementary methods that $f_m(X) \in A[X]$ (i.e. has integer coefficients) and that for $\deg(m) > 1$, we have $\deg(f_m(X)) = \frac{\varphi(m)}{r-1}$. Moreover, $\Phi_m(X) = f_m(X^{r-1})$, because (after simplifying the right-hand side) the polynomials on both sides are monic, are of degree $\varphi(m)$, and have λ as a root. Now on comparing this with $\Phi_m(X)$, we have, $f_m(X) = X^s + a_{s-1}X^{s-1} + \dots + a_1X \pm 1$ where $s = \frac{\varphi(m)}{r-1}$ and $a_i \in A$. So,

$$\Phi_m(X) = f_m(X^{r-1}) = \left(\sum_{i=1}^s a_i X^{i(r-1)} \right) + 1 \quad \text{with } a_s = 1.$$

The middle coefficient of $\Phi_m(X)$ is $a_m^+(\frac{s}{2})$, the coefficient of $X^{\frac{s}{2}}$ in $f_m(X)$. This integer is simply the middle coefficient of $f_m(X)$.

□

Over \mathbb{F}_2 , the degree of all cyclotomic polynomials is odd and so the above result does not hold. For this reason, we needed $r \equiv 1 \pmod{2}$. In the case where $r \equiv 0 \pmod{2}$, we either have no middle coefficient or there are two possible coefficients depending one's interpretation. This is similar to the classical situations, $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$. In fact, over $A = \mathbb{F}_2[T]$, one can show that there is only one root of $\phi_m(X)$ with valuation $\deg(m) - 2$ (with respect to ∞). Implying there is no middle coefficient or there are exactly 1 and $\hat{\lambda}$. (of course considering the middle two coefficients since $\deg(\Phi_m(X))$ is odd)

By using the theory of cyclotomic polynomials and extensions, one can establish another proof of the function field (polynomial) version of the quadratic reciprocity law by Carlitz.

In summary,

¹At this link: <http://mathworld.wolfram.com/CyclotomicPolynomial.html>, I came across a compelling recursive formula implemented in Wolfram Mathematica that computes numerically the coefficients of classical cyclotomic polynomials. Unfortunately no proof nor reference to the proof was given, however, A. Grytczuk and B. Tropic have a given a proof, but still cannot find their paper. I hope, a thorough understanding of this formula will give heights of classical cyclotomic polynomials either explicitly or asymptotically.

Number fields (\mathbf{Q})	Rational function field (k)
$a, b, d, n \in \mathbf{Z}, \alpha = 1, 2$	$a, b, m, d \in A, \alpha \in \mathbf{F}_r^*$
$\#\mu_n = \varphi(n)$	$\#\Lambda_m = \varphi(m)$
$d n \Leftrightarrow \mu_d \subset \mu_n$	$d m \Leftrightarrow \Lambda_d \subset \Lambda_m$
$\zeta_n \in \mu_n, a \in \mathbf{Z}, \text{ then } \zeta_n^a \in \mu_n$	$\lambda \in \Lambda_m, a \in A, \text{ then } \phi_a(\lambda) \in \Lambda_m$
$a \equiv b \pmod{n} \Leftrightarrow \zeta_n^a = \zeta_n^b$	$a \equiv b \pmod{m} \Leftrightarrow \phi_a(\lambda) = \phi_b(\lambda)$
$\text{Gal}(K_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*$	$\text{Gal}(K_m/k) \cong (A/mA)^*$
Proposition 1.2.1	Proposition 5.2.1
Proposition 1.2.2	Proposition 5.2.6
Proposition 1.2.3	Theorem 5.2.9
Corollary 1.2.4	Theorem 5.2.11
Proposition 1.2.6	Proposition 5.2.12
Proposition 1.2.7	Observation 5.2.13
Proposition 1.2.5	Theorem 5.2.15
Theorem 1.3.1	Conjecture 5.3.1
$\Phi_{n \neq \alpha p^s}(0) = 1$ and $\overline{\Phi_{\alpha p^s}}(0) = p$	Proposition 5.3.20
? ¹	$h(\alpha) = 0$ and $h(m) = \sum_{d_+ m} r^{\deg(d_+)-1} \mu(\frac{m}{d_+})$
$\mathcal{A}(\alpha p^s) = s$	$\mathcal{A}(\alpha P^s) = (r^{\deg(P)} - 1)(s - 1)$
\vdots	\vdots

Table 5.1. Analogy between the classical and Carlitz cyclotomic polynomials

Chapter 6

Mahler measure

In this chapter, we shall review what Mahler measure is, state some of its elementary properties and calculate explicitly the Mahler heights of $\phi_m(X)$ and $\Phi_m(X)$. In this setting, we replace the usual absolute value in \mathbf{R} with the absolute value coming from the place at ∞ .

6.1 Elementary properties of Mahler measure

Definition 6.1.1. Suppose $f(z) \in \mathbf{C}[z]$, then $f(z)$ factors as $f(z) = \alpha(z - \alpha_1) \cdots (z - \alpha_n)$ over \mathbf{C} . The Mahler measure of $f(z)$ with respect to the usual absolute value $|\cdot|$ is given by

$$\mathcal{M}(f) = |\alpha| \prod_{i=1}^n \max\{1, |\alpha_i|\},$$

or equivalently as a logarithmic Mahler measure,

$$m(f) = \ln(|\alpha|) + \sum_{i=1}^n \ln(\max\{1, |\alpha_i|\}) = \ln(\mathcal{M}(f)).$$

It is easy to show that Mahler measure as a ‘measure’ is multiplicative, so it makes sense to talk about the Mahler measure of rational functions. Note, for monic polynomials, we observe that $\mathcal{M}(f) \geq 1$. The term Mahler height (or ‘measure’) was first coined by Waldschmidt [23] to distinguish it from the naive or the classical notion of height, but later Boyd [7] and Durand [9] interpreted the function as a measure rather than the name.

Proposition 6.1.2. Let $s \in \mathbf{Z}$, $f(z) \in \mathbf{C}[z]$, then $\mathcal{M}(f(z)) = \mathcal{M}(f(-z)) = \mathcal{M}(f(z^s))$.

6.2 Mahler measure for Carlitz's polynomials

In comparison with the classical Mahler measure, we choose and take our valuations with respect to the place ∞ (this corresponds to $\frac{1}{T}$), and consider the absolute value associated to this valuation. Suppose now $f(z) \in \mathbf{C}_\infty[z]$, then f factors as $f(z) = \alpha(z - \alpha_1) \cdots (z - \alpha_n)$ over \mathbf{C}_∞ where $\alpha \in \mathbf{C}_\infty^*$. We define the Mahler measure of $f(z)$ with respect to $|\cdot|_\infty$ as

$$\mathcal{M}(f) = |\alpha|_\infty \prod_{i=1}^n \max\{1, |\alpha_i|_\infty\}.$$

Through out this section, we take f to be monic and therefore $\mathcal{M}(f) = \prod_{i=1}^n \max\{1, |\alpha_i|_\infty\}$.

Since Mahler measure is multiplicative, proposition 5.2.1 shows that to determine Mahler measure of a Carlitz polynomial, it suffices to find Mahler measure of its Carlitz cyclotomic factors. Since all roots of the Carlitz cyclotomic polynomials are conjugate, they must have the same norm and therefore absolute value. So, in principle it is enough to find the norm of any generator of Λ_m as an A -module. We therefore have the following propositions.

Proposition 6.2.1. *Let $a \in A$ be of order ≥ 2 , then $\mathcal{M}(\Phi_a) = 1$.*

Proof. Proposition 5.4.2 asserts that, if $a \in A$ is composite, then the generators of Λ_a are units, therefore all the conjugates are units (have absolute value 1) hence $\mathcal{M}(\Phi_a) = 1$. \square

This is analogous to the classical result, whereby $\mathcal{M}(g) = 1$ if and only if atleast one of the roots of $g(x)$ lies on (others may lie inside) the unit circle. If this is the case, then classically g is said to be cyclotomic (i.e. 'circle dividing'). Over the function fields, we instead say g is a division polynomial (if its Mahler measure is 1). We now discuss the Mahler measure of the order 1 cyclotomic polynomials, since they are Eisenstein.

Proposition 6.2.2. *Let $P \in A^+$ be a prime polynomial, then $\mathcal{M}(\Phi_P) = |P|$.*

Proof. Proposition 5.4.2 asserts that for every prime $P \in A$, with λ as a generator of the $\phi_P(X)$ torsion points, we have $\frac{\phi_b(\lambda)}{\lambda} \in \mathcal{O}_P^*$ for all $b \in A$ co-prime to P . Since all these P -torsion points are non-zero algebraic functions, moreover non units, their norms in k must be different from 0 and 1 i.e. their absolute values are strictly greater than 1. Thus,

$$\mathcal{M}(\Phi_P) = \prod_{i=1}^{\varphi(P)} \max\{1, |\lambda_i|\} = |P^{\frac{1}{[k_P:k]}}|^{\varphi(P)} = |P^{\frac{1}{\varphi(P)}}|^{\varphi(P)} = |P|.$$

\square

Corollary 6.2.3. *Let $s \in \mathbf{N}$ and $P \in A$ be a prime, then $\mathcal{M}(\Phi_{Ps}) = |P|$.*

Proof. Follows from proposition 5.3.20. \square

Corollary 6.2.4. *Let $m \in A^+$, then $\mathcal{M}(\phi_m) = |m| = r^{\deg(m)}$.*

Proof. Follows from the fact Mahler measure is multiplicative and proposition 6.2.1. □

The height of any element of A is of the form r^n , where $n \in \mathbf{Z}_{\geq 0}$. If for some $f \in A[X]$, $\mathcal{M}(f) = r^n$, then, the product of all the non-zero roots of f is equal to some $m \in A$. Considering all the non zero roots of f , gives we get some form of Carlitz polynomial; so combining propositions 6.2.1, 6.2.2 with corollaries 6.2.3 and 6.2.4, we obtain the theorem below.

Theorem 6.2.5. *If $g(X) \in A^+[X]$, $\alpha \in \mathbf{F}_r^*$, then if $g(X)$ is a product of powers of $X - \alpha$ and Carlitz cyclotomic polynomials, then $\mathcal{M}(g) = r^n$ for some $n \in \mathbf{N}$.*

This is analogous to the forward part of the following classical theorem due to Kronecker,

Theorem 6.2.6 (Kronecker's theorem). *If $f(x) \in \mathbf{Z}[x]$ is monic, then $\mathcal{M}(f) = 1$ if and only if $f(x)$ is a product of cyclotomic factors and x .*

I am still searching the complete analogue to this classical theorem.

6.3 Mahler measure for *classical* Eisenstein forms

In the classical case, we recall that all roots of cyclotomic polynomials are roots of unity and therefore lie on the unit circle and so the Mahler measure of any classical cyclotomic polynomial is 1. In this respect, the Mahler measure gives the average height of the roots of the polynomial away from the unit circle. An interesting case occurs for order 1 cyclotomic polynomials which are well known to have Eisenstein forms. It turns out that these polynomials no longer have $\mathcal{M}(f) = 1$. In fact none of them for $p > 2$ has any root of unity as a zero.

Proposition 6.3.1. *Let p be an odd prime, then*

$$\mathcal{M}(\widehat{\Phi}_p) = 2^{2a[p]} \prod_{j=1}^{a[p]} \cos^2\left(\frac{\pi j}{p}\right), \text{ where } a[p] = \lfloor \frac{\varphi(p)}{3} \rfloor.$$

Proof. Clearly $\Phi_p(X) = X^{p-1} + \dots + X + 1$ and its Eisenstein form is $\widehat{\Phi}_p(X) = \Phi_p(X + 1)$. Observe that the roots of $\widehat{\Phi}_p(X)$ are $1 + \zeta_p^a$, where $a = 1, \dots, p - 1$ and ζ_p is the p^{th} root of unity. Also when we consider the unit circle, for $p \geq 3$, the roots of $\Phi_p(X)$ occur in conjugate pairs, therefore it suffices to consider those cases where $|1 + \zeta_p^s| \geq 1$ (i.e. all those roots that are mapped onto the major arc of the unit circle centred at $(1, 0)$ subtending an angle of 240°). Observe that, when $p \equiv 1, 3 \pmod{4}$, then we have $2 \lfloor \frac{\varphi(p)}{3} \rfloor$ roots of $\Phi_p(X)$ on the major arc AB , of the unit circle centred at $(1, 0)$ as shown in figure 6.1 i.e those such that $|1 + \zeta^s| \geq 1$,

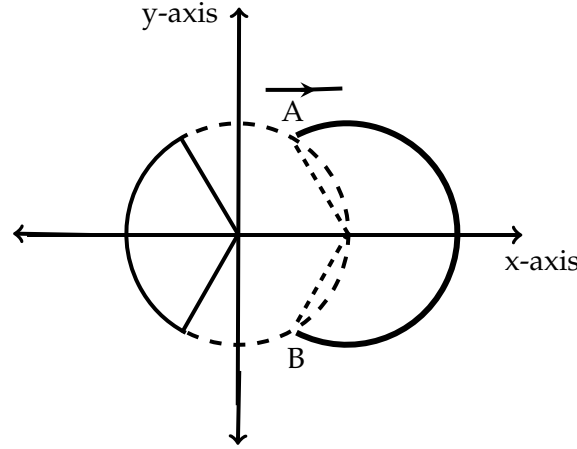


Figure 6.1. Major arc AB of the unit circle shifted to the right by a unit.

therefore $s = 1, \dots, \lfloor \frac{1}{3}\varphi(p) \rfloor, p-1 - \lfloor \frac{1}{3}\varphi(p) \rfloor, \dots, p-1$. Now since roots of unity always occur in conjugate pairs, it suffices to consider $s = 1, \dots, \lfloor \frac{1}{3}\varphi(p) \rfloor$.

$$\begin{aligned} \mathcal{M}(\widehat{\Phi}_p) &= \prod_{j=1}^{p-1} \max\{1, |1 + \zeta^j|\} = \prod_{j=1}^{a[p]} |1 + \zeta^j| \prod_{j=1}^{a[p]} |1 + \zeta^{-j}| \\ &= \prod_{j=1}^{a[p]} |(2 + \zeta^j + \zeta^{-j})| = \prod_{j=1}^{a[p]} 4 \cos^2\left(\frac{\pi j}{p}\right). \end{aligned}$$

□

Corollary 6.3.2. *Let $s \in \mathbf{N}$, then*

$$\mathcal{M}(\widehat{\Phi}_{p^s}) = \prod_{j=1, (j, p^s)=1}^{a[p^s]} 4 \cos^2\left(\frac{\pi j}{p^s}\right), \text{ where } a[p^s] = \lfloor \frac{p^s}{3} \rfloor.$$

Proof. The formula for $a[p^s]$ comes from counting of roots of unity in the first trisection of the unit circle and then the Mahler measure formula in corollary 6.3.2 sieves out the non-primitive p^s roots of unity by taking on only those j 's that are co-prime to p^s . The remaining factor is got by taking into account the fact that all the primitive roots of unity for $n \geq 3$ occur in conjugate pairs and the calculation in the proof of proposition 6.3.1. □

Corollary 6.3.3. *Let $s \in \mathbf{N}$, then $\mathcal{M}(\widehat{\Phi}_{2p^s}) = \mathcal{M}(\widehat{\Phi}_{p^s})$.*

Proof. The proof of this corollary follows from the fact that $\Phi_{2n}(X) = \Phi_n(-X)$ and that $\widehat{\Phi}_{2n}(X) = \Phi_{2n}(X-1)$ (This is just a reflection of Figure 6.1 through the y -axis). □

We illustrate this in the following examples;

1. Consider $s = 2$ and $p = 3$, then $\Phi_9(X) = \Phi_3(X^3) = X^6 + X^3 + 1$ and its Eisenstein form is actually $\widehat{\Phi}_9(X) = \Phi_9(X + 1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$. We calculate its Mahler measure; we have $a[9] = 3$

$$\mathcal{M}(\widehat{\Phi}_9) = 2^4 \cos^2\left(\frac{\pi}{9}\right) \cos^2\left(\frac{2\pi}{9}\right) \approx 8.2909.$$

Explicitly, the roots of $\Phi_9(x)$ are $\approx -0.93969 \pm 0.34202i, 0.17365 \pm 0.98481i, 0.76604 \pm 0.64279i$; those of $\widehat{\Phi}_9(x)$ are $0.06031 \pm 0.34202i, 1.17365 \pm 0.98481i, 1.76604 \pm 0.64279i$. The non-effective roots (those that do not contribute anything) in the Mahler measure calculation are $0.06031 - 0.34202i$ and $0.06031 + 0.34202i$. So,

$$\begin{aligned} \mathcal{M}(\widehat{\Phi}_9) &\approx |1.17365 - 0.98481i| \cdot |1.76604 - 0.64279i| \cdot \\ &\quad |1.17365 + 0.98481i| \cdot |1.76604 + 0.64279i| \\ &\approx 8.2909. \end{aligned}$$

2. Consider $s = 2$ and $p = 5$, then $\Phi_{5^2}(X) = \Phi_5(X^5) = X^{20} + X^{15} + X^{10} + X^5 + 1$ and its Eisenstein form is actually $\widehat{\Phi}_{25}(X) = X^{20} + 20X^{19} + \dots + 50X + 5$. In this case, the Mahler measure is computed as follows. We have $a[25] = 8$ and so,

$$\mathcal{M}(\widehat{\Phi}_{25}) = 2^{12} \cos^2\left(\frac{\pi}{25}\right) \cos^2\left(\frac{2\pi}{25}\right) \cos^2\left(\frac{3\pi}{25}\right) \cos^2\left(\frac{4\pi}{25}\right) \cos^2\left(\frac{6\pi}{25}\right) \cos^2\left(\frac{7\pi}{25}\right) \cos^2\left(\frac{8\pi}{25}\right) \approx 155.7$$

This can be verified by computing the roots of $\widehat{\Phi}_{25}(X)$ (up to 4 decimal places), then calculating $\mathcal{M}(\widehat{\Phi}_{25})$ using the definition. However, this approach is cumbersome.

We have been unable to provide interesting examples for this since my computer crashed.

Chapter 7

Conclusion

In this thesis, we investigated the analogues of classical cyclotomic polynomials over the rational function field $\mathbf{F}_r(T)$. We used the theory of Carlitz module to define $\phi_a(X)$, $\Phi_a(X)$, mainly followed the discussion in chapter 1 to explore their elementary properties and coefficients. We stated and proved the analogues of propositions 1.2.1, 1.2.3, 1.2.4, 1.2.5 and 1.2.6.

Our attempts to find the full analogue to theorem 1.2.7 (i.e. palindromy of the coefficients of $\Phi_m(X)$) failed because $\text{Char}(k) = p > 0$, $\phi(m)$ is in general NOT a p -power and $\phi_m(X)$ is not reciprocal. Imitating the classical notion of order and the number-function field analogy, we defined order, and height of Carlitz cyclotomic polynomials. Much as these notions yielded no interesting results, we were able to obtain an expression for computing the logarithmic heights of $\Phi_m(X)$ but the classification of the polynomials according to order was lost. We also found that, $h(\Phi_m(X))$ grows exponentially with the degree of m compared to the order of $\Phi_m(X)$ as opposed to the classical case where the size of n does not matter but the order of $\Phi_n(X)$. Motivated by classical results, we defined ‘prime height’ for order 1 cyclotomic polynomials. This helped us restore the analogy between classical and Carlitz cyclotomic polynomials of order 1. see theorems 5.3.12 and 5.3.16. A quick proof to a special case of Dirichlet’s theorem on primes in an arithmetic progression was given. see Theorem 5.3.22.

Again motivated by classical results, we extended the definition of Mahler measure of classical cyclotomic polynomials to Carlitz cyclotomic polynomials and calculated Mahler measures of $\Phi_m(X)$ and $\phi_m(X)$. In this way, we attempted to give the analogue of the classical Kronecker theorem. We used some results from this to again explore more about Mahler measures of classical cyclotomic polynomials. In here, we obtained a formula for computing the Mahler measure of Eisenstein forms of classical cyclotomic polynomials.

We only studied coefficients of order one cyclotomic polynomials, but we hope to further research on coefficients and heights of higher order polynomials. We would also like to

know whether the coefficients of these polynomials are of any arithmetic significance. As a corollary to proposition 5.3.20, each prime in A appears as coefficient in some cyclotomic polynomial. Also since $\phi'_m(X) = m$, A is the set of coefficients of Carlitz polynomials. This evidence together with the polynomial version of the Prime number theorem compelled us to conjecture that, *'the set of all coefficients of cyclotomic polynomials over k is A '*.

In chapter 5, we saw that using the Carlitz action one would generate a Carlitz triangle more less similar to the Pascal's triangle whose arithmetic is worth investigating. Actually it turns out that some classical properties embedded in the Pascal's triangle also have analogues over the function fields. (This is our current micro-project, 2011). We do not yet know whether such nice things exist for Drinfeld modules of arbitrary rank. Another item worth of investigation is the divisibility of $\Phi_m(X)$ over prime moduli, that is to say, finite fields of the form A/PA . Could this also shed more light on how to factor bivariate polynomials over k using Carlitz cyclotomic polynomials? Lastly, studying these polynomials in towers of Galois fields and of course how they factorise in these towers would also be interesting.

Chapter 8

Appendix

8.1 Algorithms

Notation:

$a, m, s \in A^+$ and P is a prime in A .

$\phi_a(X)$ is the Carlitz polynomial corresponding to a .

$\phi_{a_i}(X)$ = part of $\phi_a(X)$ with terms from the 1st up to the i^{th} term.

$\Phi_a(X)$ is the Carlitz cyclotomic polynomial corresponding to a .

Algorithm 1 Computing $\phi_P(X)$ by a recursion formula

Input: P with $n = \deg(P) \geq 1$

Output: $\phi_P(X)$

1. $a_0 \leftarrow P$
2. $\phi_{a_0}(X) \leftarrow PX$
3. for $i = 1$ to n
4. $a_i \leftarrow \frac{a_{i-1}^r - a_{i-1}}{T^{r^i} - T}$
5. $\phi_{a_i}(X) \leftarrow a_i X^{r^i} + \phi_{a_{i-1}}(X)$
6. $\phi_P(X) \leftarrow \phi_{a_n}(X)$

Return: $\phi_P(X)$

Algorithm 2 Computing $\phi_m(X)$ by repeated polynomial division

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$ where $e_i > 0$ for all $1 \leq i \leq t$ **Output:** $\phi_m(X)$

1. $a \leftarrow 1$
2. $\phi_a(X) \leftarrow X$
3. for $i = 1$ to t
4. $\phi_{aP_i}(X) \leftarrow \phi_a(\phi_{P_i}(X))$
5. $a \leftarrow aP_i$
6. $s \leftarrow \frac{m}{a}$
7. $\phi_m(X) \leftarrow \phi_a(\phi_s(X))$

Return: $\phi_m(X)$

Algorithm 3 Computing $\Phi_m(X)$ by repeated polynomial division

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$ where $e_i > 0$ for all $1 \leq i \leq t$ **Output:** $\Phi_m(X)$

1. $a \leftarrow 1$
2. $\Phi_a(X) \leftarrow X$
3. for $i = 1$ to t
4. $\Phi_{aP_i}(X) \leftarrow \frac{\Phi_a(\phi_{P_i}(X))}{\Phi_a(X)}$
5. $a \leftarrow aP_i$
6. $s \leftarrow \frac{m}{a}$
7. $\Phi_m(X) \leftarrow \Phi_a(\phi_s(X))$

Return $\Phi_m(X)$

Appendix B

8.2 Eisenstein forms of order one cyclotomic polynomial

Definition 8.2.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbf{Z}[x]$. $f(x)$ is said to be an Eisenstein polynomial if there exists prime p such that (i) p divides a_i for $i = 0, 1, \dots, n-1$ and (ii) p does not divide a_0^2 . e.g. $g(x) = x^2 + p^na x + p$ for any $a \in \mathbf{Z}$ is Eisenstein for the prime p .

An irreducible polynomial $f(x)$ is said to have an Eisenstein form, if it can be turned into (shifted to) an Eisenstein polynomial of the same degree and leading coefficient by an algebraic transformation. In fact for our cyclotomic polynomials, we shall only use linear transformations. Shortly, we will show that, all prime cyclotomic polynomials have Eisenstein forms. It is these new polynomials that we call the Eisenstein-cyclotomic polynomials (much as their roots are not necessarily roots of unity) or simply ‘Eisenstein forms’ and denote them with hats e.g. the Eisenstein form corresponding to $\Phi_p(X)$ is $\widehat{\Phi}_p(X)$.

Proposition 8.2.2. All order one cyclotomic polynomials have ‘Eisenstein forms’.

Proof. We consider 3 cases.

Suppose $n = p > 2$ is a prime, $\widehat{\Phi}_p(X) = \Phi_p(X+1) = X^{-1} \sum_{i=1}^p \binom{p}{i} X^i = X^{p-1} + \dots + p$ is the Eisenstein form required in this case, since p divides $\binom{p}{i}$ for $i = 1, \dots, p-1$ and p^2 does not divide p . Suppose $n = 2p$, where $p > 2$ is a prime. By proposition 1.2.6, we have $\Phi_{2p}(X) = \Phi_p(-X)$ hence $\Phi_{2p}(X)$ has an Eisenstein form (since -1 is a unit in \mathbf{Z}). In fact, $\widehat{\Phi}_{2p}(X) = \Phi_{2p}(X-1) = \Phi_p(-X+1)$, is the required form (the substitution $X-1$ makes every coefficient positive). Lastly, suppose $n = 2^s p^t$ where $s \in \mathbf{N}_{\geq 2}$ and $t \in \mathbf{Z}^+$, then clearly, we have $\widehat{\Phi}_{2^s p^t}(X) = \Phi_{2p}(X^{2^{s-1} p^{t-1}})$. By case 2 above, proposition 5.2.12 is established. \square

Definition 8.2.3. Let $f = \sum_{i=0}^n a_i x^i \in \mathbf{Q}[x]$, set $\mathcal{H}_p(f) := \max\{|a_i|_p : \text{for } 0 \leq i \leq n\}$, where $|a|_p$ is the p -adic absolute value of a . We set $\mathcal{H}_\infty := \mathcal{H}$, i.e. the usual absolute value in \mathbf{R} .

For order one cyclotomic polynomials, we set $\widehat{\Phi}_{p^s}(X)$ and $\widehat{\Phi}_{2^s p^t}(X)$ to be the associated Eisenstein forms respectively. $\mathcal{A}(n) := \text{Log}_p(\mathcal{H}_p(\widehat{\Phi}_n(X)))$, where p is the unique odd prime dividing n is called the prime height of $\Phi_n(X)$. In other words, $\mathcal{A}(p)$ is like a ‘measure’ of

divisibility of coefficients of $\widehat{\Phi}_p(X)$ with respect to p . In order to calculate $\mathcal{A}(p^t)$, $\mathcal{A}(2p^t)$, we first transform $\Phi_p(X)$ into $\widehat{\Phi}_p(X)$. We denote the height of $\widehat{\Phi}_n(x)$ by $\widehat{\mathcal{H}}(n)$ or $\mathcal{H}(\widehat{\Phi}_n(x))$.

Theorem 8.2.4 (Legendre, 1808). *Let p be a prime and let $n = a_0p^t + a_1p^{t-1} + \cdots + a_{t-1}p + a_t$ be the base p expansion of n . The exact power m of p dividing $n!$ is given by*

$$v_p(n!) = \frac{n - (a_0 + a_1 + \cdots + a_t)}{p - 1}. \quad (8.1)$$

Lemma 8.2.5. *Let $t \in \mathbf{Z}^+$, then $0 \leq v_p\left(\binom{p^t}{x}\right) \leq t$. If $x \not\equiv 0 \pmod{p}$, then $v_p\left(\binom{p^t}{x}\right) = t$.*

Proof. Let $g(x) = \binom{p^t}{x} = \frac{p^t!}{(p^t-x)!x!}$, where $x \in \mathbf{N}$. Now, since $g(x) \in \mathbf{Z}$, we have $v_p(g(x)) \geq 0$. Also $v_p(g(x)) = v_p(p^t!) - v_p((p^t - x)!) - v_p(x!)$. By symmetry of the binomial coefficients, it is enough to consider valuations for $x \leq \lfloor \frac{p^t}{2} \rfloor$. Clearly, $v_p(g(0)) = 0$ and $v_p(g(1)) = t$. This follows from considering the following facts (obtained using theorem 8.2.4)

1. $g(0) = 1$,
2. $v_p(p^t!) = \frac{p^{t+1}-1}{p-1}$,
3. if $x = ap^s$ where $0 \leq a \leq p-1$, then $v_p(x!) = a \frac{p^{s+1}-1}{p-1}$,
4. if $x = ap^s$, $0 \leq a \leq p-1$, $1 \leq s \leq t-1$, then $v_p((p^t - x)!) = \frac{p^{t+1}-1}{p-1} - a \frac{p^{s+1}-1}{p-1} - (t-s)$.

Claim: If $x \equiv 0 \pmod{p}$, then $v_p(g(x)) \leq t-1$, otherwise $v_p(g(x)) = t$.

1. When $x \equiv 0 \pmod{p}$, in particular for $x = ap^s$ with $s \leq t-1$ and $1 \leq a \leq p-1$, we then have $v_p(x!) = v_p(ap^s!) = a \frac{p^{s+1}-1}{p-1}$. Therefore, $0 \leq v_p(g(x)) \leq t-1$.
2. Otherwise, take $x = ap^s + \alpha$, where $1 \leq \alpha, a \leq p-1$. In this case, $v_p(x!) = a \frac{p^{s+1}-1}{p-1}$, since all the first α factors in the factorial expansion of $x!$ have (each) valuation 0. By a similar reasoning to $(p^t - x)!$, we get $v_p((p^t - x)!) = \frac{p^{t+1}-1}{p-1} - a \frac{p^{s+1}-1}{p-1} - t$. Therefore, $v_p((p^t - x)!x!) = \frac{p^{t+1}-1}{p-1} - t$, and we get $v_p(g(x)) = v_p(p^t!) - v_p((p^t - x)!x!) = t$.

This completes the proof. □

Theorem 8.2.6 (Result 1). *We have $\widehat{\mathcal{H}}(2) = 2$. For $s \in \mathbf{N}$, we have $\widehat{\mathcal{H}}(2^s) = \binom{2^{s-1}}{2^{s-2}}$ and*

$$\widehat{\mathcal{H}}(p^s) = \begin{cases} \binom{p}{\frac{p-1}{2}}, & \text{if } p > 2 \text{ and } s = 1, \\ \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}, & \text{if } p > 2 \text{ and } s > 1. \end{cases}$$

Proof. This is based on the fact that the maximum coefficient in a binomial expansion is the coefficient of the middle term. We shall do this in 3 steps as follows,

1. When $p = 2$, we have $\Phi_2(X + 1) = X + 2$, thus $\hat{\mathcal{H}}(2) = 2$. For $s > 1$, we get $\Phi_{2^s}(X + 1) = (X + 1)^{2^{s-1}} + 1$, whose maximum absolute coefficient is $\hat{\mathcal{H}}(2^s) = \binom{2^{s-1}}{2^{s-2}}$.
2. when $p > 2, s = 1$, we have $\Phi_p(X + 1) = \sum_{i=1}^p \binom{p}{i} X^{i-1}$. The maximum coefficient (in absolute values) is the coefficient of $X^{\frac{p-1}{2}}$ or $X^{\frac{p-3}{2}}$, so $\hat{\mathcal{H}}(p) = \binom{p}{\frac{p-1}{2}} = \binom{p}{\frac{p+1}{2}}$.
3. When p is odd and $s > 1$, then $\Phi_{p^s}(X + 1) = \Phi_p((X + 1)^{p^{s-1}}) = \sum_{i=0}^{p-1} (X + 1)^{p^{s-1}i}$. Even heuristics show that $\hat{\mathcal{H}}(p^s)$ is the middle term in $\Phi_{p^s}(X + 1)$. Therefore, we have $\hat{\mathcal{H}}(p^s) X^{\frac{\phi(p^s)}{2}} = \sum_{i=0}^{p-1} \sum_{j=0}^{p^{s-1}i} \chi_0(j) \binom{p^{s-1}i}{j} X^j$, where $\chi_0(j) = 1$ if $j = \frac{\phi(p^s)}{2}$, and 0 otherwise. With the help of this sieve, the coefficients of $X^{\frac{\phi(p^s)}{2}}$ are of the form $\binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}$. This restricts us to values of $i \geq \frac{p-1}{2}$, therefore $\hat{\mathcal{H}}(p^s) = \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}$.

□

Corollary 8.2.7. *Let $s \in \mathbf{Z}^+$, then $\mathcal{A}(p^s) = s$ and $\mathcal{A}(2p^s) = s$.*

Proof. By lemma 8.2.5 $\Phi_{p^s}(X + 1) = \sum_{i=0}^{p-1} (X + 1)^{p^{s-1}i}$ is Eisenstein, it suffices to consider, the valuation of coefficient of X in $\Phi_{p^s}(X + 1)$, so $\mathcal{A}(p^s) = v_p \left(\sum_{i=1}^{p-1} \binom{p^{s-1}i}{1} \right) = v_p(p^{s-1} \sum_{i=1}^{p-1} i) = s$. The second formula follows from proposition 1.2.6 $\mathcal{A}(p^s) = s$. □

Theorem 8.2.8 (Result 2).

$$\hat{\mathcal{H}}(2p^s) = \begin{cases} \binom{p}{\frac{p-1}{2}}, & \text{if } p > 2 \text{ and } s = 1, \\ \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}, & \text{if } p > 2 \text{ and } s > 1. \end{cases}$$

Proof. We do this in 2 steps, since it is trivial for $p = 2$ and $s \geq 1$.

1. For $p > 2$ and $s = 1$, $\Phi_{2p}(X - 1) = \sum_{i=1}^p \binom{p}{i} (-X)^{i-1}$. Therefore, $\hat{\mathcal{H}}(2p) = \binom{p}{\frac{p-1}{2}}$.
2. For $p > 2$ and $s > 1$, then $\Phi_{2p^s}(X - 1) = \Phi_{p^s}(-X + 1) = \sum_{i=0}^{p-1} (-X + 1)^{p^{s-1}i}$. Similar arguments as in theorem 8.2.6 give the desired result.

□

Example 8.2.9. *Take $p = 3$, and $s = 4$, then $\Phi_{3^4}(X) = \Phi_3(X^{27}) = X^{54} + X^{27} + 1$. Its Eisenstein form is $\widehat{\Phi}_{3^4}(X) = \Phi_{3^4}(X + 1) = X^{54} + 54X^{53} + 1431X^{52} + 24804X^{51} + \dots + 333801X^4 + 27729X^3 + 1782X^2 + 81X + 3$. The set of 3-adic valuations of all the coefficients in ascending powers of X is $[1, 4, 4, 3, 4, \dots, 2, 3, 3, 0]$, so $\mathcal{A}(3^4) = 4$. Moreover, $\hat{\mathcal{H}}(3^4) = 1946939425648113$ and by theorem 8.2.8, we have*

$$\hat{\mathcal{H}}(3^4) = \binom{3^3}{3^3} + \binom{2 \cdot 3^3}{3^3} = 1 + 1946939425648112 = 1946939425648113.$$

Bibliography

- [1] E. Artin and J. Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.
- [2] G. Bachmann. Flat Cyclotomic Polynomials of Order Three. *Bull. London Math. Soc.*, 38(1):53–60, 2006.
- [3] S. Bae. The arithmetic of Carlitz polynomials. *J. Korean Math. Soc.*, 35:341–360, 1998.
- [4] S. Bae and S. Hahn. On the Carlitz module. *J. Chungcheong Math. Soc.*, 4:85–90, 1991.
- [5] P. Bateman, C. Pomerance, and R. Vaughan. On the size of the coefficients of the cyclotomic polynomial. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, pages 171–202. North-Holland, Amsterdam, 1984.
- [6] M. Beiter. Coefficients of the cyclotomic polynomial $F_{3qr}(x)$. *Fibonacci Quart.*, 16(4):302–306, 1978.
- [7] D. Boyd. Speculations concerning the range of Mahler’s measure. *Canad. Math. Bull.*, 24:453–469, 1981.
- [8] L. Carlitz. On polynomials in a Galois field. *Bull. Amer. Math. Soc.*, 38:734–744, 1932.
- [9] A. Durand. On Mahler’s measure of a polynomial. *Proc. Amer. Math. Soc.*, 83:75–76, 1981.
- [10] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1996.
- [11] D. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.
- [12] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [13] N. Kaplan. Flat cyclotomic polynomials of order four and higher. *Integers*, 10:357–363, 2010.

-
- [14] T. Lam and K. Leung. On the cyclotomic polynomial $\phi_{pq}(x)$. *Amer. Math. Monthly*, 103(1):562–564, 1996.
- [15] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [16] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.
- [17] V. Prasolov. *Polynomials*. Springer-Verlag Berlin Heidelberg, 2004.
- [18] M. Rosen. *Number Theory in Function Fields*. Springer-Verlag, Berlin, New York, 2002.
- [19] G. Salvador. *Topics in the Theory of Algebraic Function Fields*. Birkhauser, Boston, 2006.
- [20] W. Stein et al. SAGE Mathematical Software Version 4.2.6, 2011.
- [21] J. Suzuki. On the coefficients of cyclotomic polynomials. *Proc. Japan Acad. Soc.*, A63:279–280, 1987.
- [22] D. Thakur. *Function field arithmetic*. World Scientific Publishing Co. Inc., River Edge, NJ, 2004.
- [23] M. Waldschmidt. Nombres transcendants et groupes algébriques. *Astérisque Société Mathématique de France, Paris*, pages 69–70, 1979.
- [24] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.